

정보보안 정책 유형과 보안 스트레스가 정보보안 행동에 미치는 영향에 대한 연구

이 광 호*, 정 찬 기**

요 약

기술 발달에 따른 기존 보안정책의 한계에도 불구하고 기업은 폐쇄적 보안정책을 유지함으로써 변화에 능동적으로 대응하지 못하고 있다. 본 연구는 정보보안 정책을 3가지 유형인 규제형 정책, 권고형 정책 그리고 고지형 정책으로 분류하였다. 분류된 각 정책의 유형은 확장된 계획행동이론을 적용하여 조직 구성원의 정보보안 정책 준수행동에 주는 영향을 규명하고 보안 스트레스의 조절효과를 살펴보았다. 각 요인들 간에 영향을 미치는 관계를 분석하기 위해서는 구조방정식모델링 기법인 SmartPLS 2.0과 SPSS 21.0을 활용하였다. 연구 결과 규제형, 권고형 그리고 고지형 정보보안 정책은 조직 구성원의 정보보안 정책 준수행동에 영향을 주었으며 보안 스트레스는 계획된 행동이론의 선행요인인 정보보안 순응태도와 정보보안에 대한 주관적 규범에 영향을 주었다. 본 연구를 통해 기업의 정보보안 정책에 다양한 유형이 적용될 수 있음과 보안스트레스가 구성원의 정보보안 행동에 영향을 줄 수 있음이 제시되었다.

A Study on the Effects of Information Security Policy Types and Information Security Stress on Information Security Behavior

Lee Kwang Ho*, Jung Chan gi**

ABSTRACT

Despite the limitations of existing security policies due to technological development, companies are unable to actively respond to changes by maintaining a closed security policy. This study classified information security policy into three types: regulatory type policy, advisory type policy, and informative type policy. For each classified policy type, the effect on the information security policy compliance behavior of organizational members was investigated by applying the extended theory of planned behavior, and the moderating effect of information security stress was investigated. SmartPLS 2.0 and SPSS 21.0, which are structural equation modeling techniques, were used to analyze the relationship affecting each factor. As a result of the study, regulatory type, advisory type, and informative type security policies affected organizational members' information security policy compliance behavior, and security stress had an effect on information security compliance attitudes and subjective norms on information security, which are prerequisites for planned behavior theory. gave. This study suggests that various types of corporate information security policies can be applied and that security stress can affect information security behaviors of members.

Key words : Information Security Policy, Extended Theory of Planned Behavior, Information Security Stress

접수일(2022년 2월 27일), 수정일(2022년 3월 21일), 게재
확정일(2022년 3월 29일)

* 육군대학

** 이주대학교 국방디지털융합학과 (교신저자)

1. 서론

국민의 보안에 대한 인식 빠르게 변하고 있으며 이것은 산업보안 분야에 상당한 영향을 미치고 있다. 그러나 기존의 폐쇄적 보안정책과 보안 인프라는 IoT 기술의 발달과 공유와 개방을 통해 산업 생태계를 키우고 발전시키는 환경에서 그 한계점을 보여주고 있다. 그러나 조직들은 폐쇄적 보안정책을 유지함으로써 변화에 능동적으로 대응하지 못하고 있으며 폐쇄적 효과의 보안정책만을 선택하는 경영진의 의사결정으로 인하여 기업이나 조직이 본래 목적을 달성하지 못하는 사례도 발생되고 있다[1].

마이크로소프트 코리아의 2019년 발표에 따르면 클라우드, IoT, AI 등의 신기술 발달에 따라 조직의 정보가 조직 내 안정망을 벗어나는 사례가 증가하고 있으며 이와 같은 현상은 기존 보안 패러다임의 한계가 분명함에 따라 보안과 생산성의 균형을 필요로 한다고 밝혔다. 또한 CIISec Report에 따르면 과도하게 폐쇄적인 보안정책은 보안 전문가들에게 과로를 야기하고 스트레스와 번아웃의 주요 원인이 되고 있으나 보안의 효과를 유지하기에는 충분하지 않은 실정이라고 밝혔다[2].

하지만 정보보안 정책의 특성이 여러 부작용을 낳고 있음에도 불구하고 조직의 정보보안 정책 관점에서 그 문제를 깊이 있게 논의한 연구는 많지 않다. 특히 보안정책의 특성을 복합적으로 고려하여 조직 내 정보보안 문제를 이론적으로 논의하고, 실증적으로 검증한 연구는 많지 않다. 따라서 본 연구에서는 조직 내부자인 구성원들의 정보보안 정책에 대한 순응 행동에 영향을 미칠 것으로 예상되는 정보보안 정책의 유형을 세분화하여 연구를 수행하였다. 본 연구의 연구질문은 첫째 조직구성원들의 정보보안 정책 유형이 태도, 주관적 규범, 인지된 행동통제에 영향을 미치는가? 둘째, 조직의 정보보안 정책 유형에 따른 보안스트레스는 태도와 주관적 규범에 영향을 미치는가에 대한 연구이다.

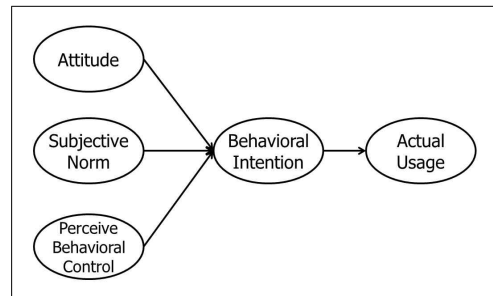
본 연구는 일반 기업 조직 구성원들을 대상으로 설문지 기법을 통해 자료를 수집하고 정보보안 정책

의 유형과 정보보안 스트레스가 정보보안 정책에 대한 순응 의도와 행동에 미치는 영향을 이론적으로 논의하고 이를 실증적으로 검증해 보고자 하였다.

2. 이론적 배경

2.1 계획된 행동이론

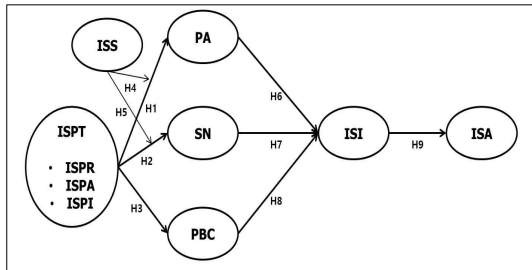
계획된 행동이론(Theory of Planned Behavior)은 합리적 행위 이론(Theory of Reasoned Action)에서 발전된 이론이다[3][4]. 합리적 행동이론의 한계는 행동에 대한 통제가 완전하지 않은 상황에서 행동에 대한 예측을 충분히 하지 못한다는 것이다[5]. 이에 따른 계획된 행동이론(TPB)은 (그림 1)과 같이 인간의 행동에서 행동의도가 중요한 요인이 되며 이 의도는 행동에 영향을 미치는 선행요인으로 적용된다[3]. 또한 의도와 행동을 유도하는 외부 변수로서 태도(attitude), 주관적 규범(subjective norm), 지각된 행동통제(perceived behavioral control)가 행동의도에 직접적인 영향을 미치며 지각된 행동통제와 행동의도는 행동에 직접적인 영향을 미친다고 보았다[4].



(그림 1) 계획된 행동이론 모델

하지만 계획된 행동이론에도 한계점이 제시되고 있는데 국내외의 계획된 행동이론의 메타분석 연구에 따르면 행동이나 행동에 대한 설명력이 30% 정도에 그치며 주관적 규범이 행동의도에 미치는 영향은 작게 나타나고, 행동의도가 행동에 미치는 영향은 상대적으로 크게 나타났다[6]. 이에 따라 계획된 행동이론의 설명력을 증대하고 행동의도에 영향을 미칠 수 있는 새로운 요인을 추가하여 그 효과를 검증하는 확장된

계획 행동이론(ETPB:Extended Theory of Planned Behavior)을 적용한 연구가 많아지고 있다[7]. 따라서 본 연구에서는 (그림 2)와 같이 정보보안 정책의 유형 (Information Security Policy Type)을 NIST가 제시한 유형에 따라 세 가지로 나누고 각각의 유형과 보안스트레스(Information Security Stress)가 정보보안 행동에 어떻게 영향을 미치는가에 대해 분석해 보았다.



(그림 2) 연구모델

2.2 조직의 정보보안 정책과 유형

조직의 정보보안 정책은 조직이 추진하는 정보보호 목표를 달성하기 위해 조직 구성원이 따라야 하는 원칙이나 규정, 지침을 포함하고 있다. 왜냐하면 조직 구성원의 정보시스템에 대한 접근과 그에 따른 정보보안 사고의 가능성 등 다양한 이유로 인해 조직의 정보를 외부로 노출 시킬 수 있기 때문이다[8]. West(2008)는 그의 연구에서 정보보안 정책의 특성에 따라 조직과 구성원의 정보보안 목표가 다를 수 있고, 보안 위험에 대해 조직 구성원의 인식에 차이가 발생하며, 조직 구성원들의 보안 행동 다르므로 정보보안 정책의 중요성을 그의 연구로 제시하였다[9].

또한 조직의 정보보안 환경에 따라 구성원에게 정보보안 행동을 요구하기 위해서는 조직이 요구하는 정보보안 수준을 명확하게 제공하는 것이 필요하다[10][11][12][13][14]. 본 연구에서는 <표 1>과 같이 정보보안 정책 유형을 NIST(2009)에서 분류한 세 가지 유형을 기준으로 분류하였다. 이를 통해 조직의 정책이 어떠한 유형의 특성에 가까운지 제시하였다.

<표 1> 정보보안 정책 유형 (NIST, 2009)

분류	내용
규제형 정책 (Regulatory Type) ISPR	1.무엇을 하여야 한다. 2.언제 하여야 한다 3.누가 하여야 한다 규제형에는 특정제한 사항이나 배제사항이 있게 되는데, 이러한 정책을 수립해 놓으면 일관성이 있고 모순이 없는 절차를 확립할 수 있다.
권고형 정책 (Advisory Type) ISPA	잘 모르는 사람에게 가르쳐 주며 정책에 맞게 하는 방법이다. 어떤 기능을 완수하기 위해서는 어떤 조치를 취하여야 한다는 권고를 하는 것이다. 때로는 강력한 제안을 포함한다.
고지형 정책 (Informative Type) ISPI	단순히 알리는 형태를 말한다. 이 정책에는 어떤 행동이 묵시적으로 기대되거나 벌칙이 없다.

Lee et al.(2004)는 그의 연구에서 정보보안 정책이 구성원의 보안 준수 의도를 높이고 남용(misuse)을 줄일 수 있는 선행요인이라고 하였으며, 조직에 맞는 정보보안 정책은 조직 구성원의 정보보안 행동에 영향을 줄 것으로 판단하였다[15][16]. 따라서 본 연구에서는 아래와 같은 가설을 제시하였다.

- H1a: 규제형 정보보안 정책은 구성원의 정보보안 순응 태도에 정(+)의 영향을 미칠 것이다
- H1b: 규제형 정보보안 정책은 구성원의 정보보안 순응에 대한 주관적 규범에 정(+)의 영향을 미칠 것이다
- H1c: 규제형 정보보안 정책은 구성원의 순응에 대한 통제에 정(+)의 영향을 미칠 것이다
- H2a: 권고형 정보보안 정책은 구성원의 정보보안 순응 태도에 정(+)의 영향을 미칠 것이다
- H2b: 권고형 정보보안 정책은 구성원의 정보보안 순응에 대한 주관적 규범에 정(+)의 영향을 미칠 것이다
- H2c: 권고형 정보보안 정책은 구성원의 순응에 대한 통제에 정(+)의 영향을 미칠 것이다
- H3a: 고지형 정보보안 정책은 구성원의 정보보안 순응 태도에 정(+)의 영향을 미칠 것이다
- H3b: 고지형 정보보안 정책은 구성원의 정보보안 순응에 대한 주관적 규범에 정(+)의 영향을 미칠 것이다
- H3c: 고지형 정보보안 정책은 구성원의 순응에 대한 통제에 정(+)의 영향을 미칠 것이다

2.3 정보보안 스트레스 (ISS)

일반적인 스트레스의 정의는 ‘특정 시점에 평가한 개인의 수요(demand)가 가용할 수 있는 자원을 초과할 때 생기며 이는 건강을 위협하고 이와 같은 불균형을 회복하기 위한 개인의 기능적 변화를 필요’로 한다 [17]. 조직 구성원들의 직접적 보안스트레스 유발 요인으로는 과도한 보안정책에 따른 프라이버시 침해(Invasion of Privacy)가 있다[18]. 하지만 조직의 정책적 특성에 따른 외부적 정보보안 스트레스는 기술적 보안 스트레스, 관리적 보안 스트레스, 물리적 보안 스트레스로 조직구성원들이 체감하는 신체적, 정서적 부정적 반응의 정도를 의미한다[19]. 조직의 이러한 정보보안 정책에 따른 정보보안 활동으로 조직구성원에 의해 인지된 감내할 수 없는 통제의 적정 수준을 넘는 경우, 이는 곧 보안스트레스의 요인이 될 수 있으며 이와 같은 요인들은 태도, 주관적 규범, 자기 효능감, 대처 효능감, 인지된 위협 민감성 등에 영향을 준다[20][21][22][23]. 따라서 본 연구에서는 아래와 같은 가설을 제시하였다.

H4a: 권고형 정보보안 정책이 정보보안 순응태도에 미치는 영향은 보안스트레스가 높은 구성원보다 낮은 구성원에게서 더 높게 나타날 것이다.

H4b: 권고형 정보보안 정책이 정보보안 순응에 대한 주관적 규범에 미치는 영향은 보안스트레스가 높은 구성원보다 낮은 구성원에게서 더 높게 나타날 것이다.

H5a: 고지형 정보보안 정책이 정보보안 순응태도에 미치는 영향은 보안스트레스가 높은 구성원보다 낮은 구성원에게서 더 높게 나타날 것이다.

H5b: 고지형 정보보안 정책이 정보보안 순응에 대한 주관적 규범에 미치는 영향은 보안스트레스가 높은 구성원보다 낮은 구성원에게서 더 높게 나타날 것이다.

2.4 정보보안 순응태도(PA), 순응에 대한 주관적 규범(SN), 순응에 대한 통제(PBC) 및 정보보안 행동(ISA)

계획된 행동이론에 의하면 개인은 행동수행과 관련하여 긍정적인 태도와 주관적 규범을 가질 뿐만 아니

라 자신이 그 행동을 수행할 수 있는 기회와 행동수행에 필요한 자원을 가진 경우 비로써 자신이 그 행동을 자신의 뜻대로 통제할 수 있다고 지각하게 되며, 이때 행동의도를 형성한다고 본다[24]. 연구에서는 Bulgurcu et al(2009)의 연구에 근거하여 ‘결과에 대한 전체적 평가에 대한 신념’이 정보보안 정책 준수에 대한 태도에 영향을 미친다고 가정하였다. 이를 연구의 주제에 맞게 적용하여 태도를 정보보안 순응 태도로, 주관적 규범을 순응에 대한 주관적 규범으로 정의하였으며 인지된 행동통제를 순응에 대한 행동통제로 정의하였다[25][26]. 이에 따라 아래와 같은 가설을 제시하였다.

H6: 정보보안 순응태도는 구성원의 정보보안 정책 순응 의도에 정(+)의 영향을 미칠 것이다.

H7: 정보보안 순응에 대한 주관적 규범은 정보보안 정책 순응의도에 정(+)의 영향을 미칠 것이다.

H8: 정보보안 순응에 대한 통제는 정보보안 정책 순응 의도에 정(+)의 영향을 미칠 것이다.

H9: 정보보안 정책 순응 의도는 정보보안 행동에 정(+)의 영향을 미칠 것이다.

3. 연구모델 및 방법

3.1 연구모델

본 연구는 (그림 2)와 같이 확장된 계획 행동이론(ETPB)을 기반으로 정보보안 정책 유형이 조직 구성원의 정보보안 정책 순응행동에 미치는 영향에 대해 접근하고 각 정보보안 정책의 유형에 따른 보안스트레스가 매개변수로써 어떤 영향을 미치는지 확인하고자 한다.

3.2 데이터 측정 및 수집방법

본 연구에서는 선행연구를 통해 측정변수들을 7점 리커트 척도를 사용하여 구성하였으며 28개의 다항목 지표들로 측정하였다. 설문은 정보보안 정책이 있는 기업 구성원을 대상으로 Google Docs로 작성된 설문조사 URL을 전송하여 진행하였으며 2022년 1월 한 달간 약 274개의 설문을 수집하여 30개의 설문을 제거하고 최종 244개의 데이터를 실제 분석하였다. 본 연구는 보안정책의 직접적인 영향을 받는 실무자들을

대상으로 데이터를 수집하여 20~30대가 94%이며 기타에는 1년 이내 퇴사 또는 육아휴직자들이 포함되어 있으나 연구대상의 선정에는 적절한 것으로 판단된다.

<표 2> 인구통계학적 특성

구분		빈도(명)	비율(%)
성별	남	144	59
	여	100	41
	소계	244	100
연령	20대	105	43
	30대	126	51
	40대 이상	13	6
	소계	244	100
직업	회사원	135	54
	공무원	50	20
	전문직	25	10
	기타	34	14
	소계	244	100
학력	전문대	54	23
	대학교	132	54
	대학원이상	58	24
	소계	244	100

4. 가설 검증

4.1 신뢰성 및 타당성 분석

<표 3> 요인분석

Construct	Factor Loading	Construct	Factor Loading
ISPR	1.000	CON2	0.925
ISPA	1.000	CON3	0.909
ISPI	1.000	CON4	0.773
ISS1	0.823	PBC1	0.869
ISS2	0.887	PBC2	0.836
ISS3	0.836	PBC3	0.920
ISS4	0.908	PBC4	0.841
ISS5	0.877	ISI1	0.916
ISS6	0.831	ISI2	0.945
PA1	0.931	ISI3	0.912
PA2	0.910	ISA1	0.918
PA3	0.933	ISA2	0.926
PA4	0.934	ISA4	0.849
CON1	0.908	-	-

본 연구에서는 SPSS 21.0과 SmartPLS 2.0을 분석에 활용하였다. 1차 확인적 요인분석 결과에서 낮게 나오는 ISA3(0.257) 항목을 제외하고 개별 측정항목들의 요인 적재량이 0.7이상으로 확인되며, 요인 적재량이 다른 변수들과 교차 요인 적재량 보다 큰 것이 확인되므로 개념타당성이 확인되었다. 측정항목의 타

당성과 신뢰도는 요인 적재치, 평균분산추출(AVE)이 0.5 이상일 때 집중타당성이 있으며, 합성신뢰도(Composite Reliabilities)는 0.7 이상, 크론바 알파(Cronbachs Alpha) 값이 0.7 이상일 때 연구 모형의 내적 일관성과 집중타당성이 확보되었다고 해석한다.

<표 4> 타당성 및 신뢰성 분석

	AVE	C. R	R. S	Crombachs alpha	Discriminant Validity	Redundancy
ISPR	1.000	1.000	-	1.000	0.942	-
ISPA	1.000	1.000	-	1.000	0.935	-
ISPI	1.000	1.000	-	1.000	0.956	-
ISS	0.741	0.945		0.930	0.741	
PA	0.861	0.961	0.720	0.946	0.861	0.169
SN	0.776	0.932	0.743	0.902	0.776	0.118
PBC	0.752	0.923	0.731	0.890	0.752	0.121
ISI	0.855	0.946	0.232	0.915	0.855	0.124
ISA	0.808	0.926	0.318	0.880	0.808	0.149

신뢰성은 크론바 알파 값이 0.6 이상일 때 신뢰성이 확보된 것으로 본다. 각 변수들 간의 상관관계를 확인하기 위한 판별타당성(Discriminant Validity)은 각 변수의 평균분산추출(AVE) 이상이고 다른 변수들의 상관계수보다 큰 것이 확인될 때 판별타당성이 확보된 것으로 보며 본 연구에서는 판별타당성이 확보되었다.

4.2 구조모형 평가 및 가설 검증

구조모형에 대한 평가는 구조모형의 통계추정량인 Redundancy의 값이 양수일 때 적합도가 있는 것으로 평가하며 R Square의 값이 0.26 이상이면 적합도가 '상', 0.13~0.26 미만 이면 '중', 0.02~0.13 미만이면 '하'로 평가한다. 본 연구에서는 Redundancy의 값이 모두 양수이며, 내생 변수의 R Square의 값은 정보보안 정책에 대한 순응의도(ISD)를 제외하고 모두 상으로 평가된다. 따라서 구조모형의 적합성이 확보되었다[27].

가설의 기각 및 채택은 t-value를 기준으로 판단할 수 있는데 그 범위를 살펴보면 1.96(P<0.005), 2.58(P<0.01), 3.29(P<0.001)이다. 세부적인 가설의 기각 및 채택 결과는 <표 5>에 요약하였다.

<표 5> 가설 검증결과

가설	경로	경로 계수	T-value	결과
H1a	ISPR → PA	0.175	2.672	채택
H1b	ISPR → PA	0.158	2.930	채택
H1c	ISPR → PA	0.253	3.587	채택
H2a	ISPA → PN	0.330	5.026	채택
H2b	ISPA → PN	0.025	4.732	채택
H2c	ISPA → PN	0.278	6.186	채택
H3a	ISPI → ISI	0.560	14.321	채택
H3b	ISPI → ISI	0.293	3.404	채택
H3c	ISPI → ISI	0.221	2.397	채택
H4a	ISPR → ISS → PA	0.342	4.826	채택
H4b	ISPR → ISS → SN	0.213	6.136	채택
H5a	ISPA → ISS → PA	0.420	10.132	채택
H5b	ISPA → ISS → SN	0.253	3.003	채택
H6	PA → ISI	0.331	2.887	채택
H7	SN → ISI	0.241	3.726	채택
H8	PBC → ISI	0.171	1.830	채택
H9	ISI → ISA	0.298	3.997	채택

5. 결 론

본 연구는 확장된 계획 행동이론(ETPB)을 기반으로 정보보안 정책의 유형이 조직 구성원들의 정보보안 정책에 대한 순응의도와 정보보안 정책 순응행동에 미치는 영향을 연구하였다. 특히 정보보안 정책의 유형을 규제형, 권고형, 고지형으로 분류하고 각각의 정보보안 정책 유형에 따른 보안 스트레스가 정보보안 순응태도와 정보보안 순응에 대한 주관적 규범에 영향을 줄 수 있음을 증명하였다. 또한 다음과 같은 시사점을 제시한다. 각각의 정보보안 정책의 유형이 계획된 행동이론의 선행요인에 영향을 줌으로써 조직 또는 기업의 유형에 따른 능동적인 보안정책이 필요하다는 것이다. 특히 서론에서 제시된바와 같이 단순하게 폐쇄적인 규제형 정책이 아닌 권고형 정책 및 고지형 정책도 조직 구성원들의 보안정책 준수 의도와 행동에는 긍정적인 영향을 줄 수 있다는 것이다. 또한 조직의 과도한 정보보안 정책 활동에 따른 구성원들의 보안 스트레스는 정보보안 순응태도와 정보보안 순응에 대한 주관적 규범에 영향을 줌으로써 결과적으로는 정보보안 정책 준수의도와 준수행동에 영향을 줄 수 있다는 것을 시사한다.

하지만 다음과 같은 한계점을 가진다. 첫째 각 조직의 보안정책의 유형을 개인이 평가함으로써 기업

특성에 따른 정책 유형을 객관적으로 반영하지 못하였다. 따라서 향후 연구에서는 조직이나 기업을 그룹화하여 조직에 대한 정책유형을 평가하고 구성원들에 대한 표본을 조직이나 기업 단위로 구분하여 비교분석할 필요가 있다. 둘째로 본 연구는 정보보안 정책의 유형과 보안스트레스의 강도 간의 관계 및 그에 따른 조절변수로서의 효과를 반영하지 못하였다. 따라서 향후 연구에서는 이에 대한 새로운 접근 방법을 제시할 수 있을 것으로 판단된다.

참고문헌

- [1] 노광태 & 이민화(2016), “산업 패러다임변화와 보안정책 의사결정모델에 대한 연구”, 한국경영학회 통합학술발표논문집, 2016.08, pp.2305-2318.
- [2] Industry Survey White Paper(2021), CIISec Report
- [3] Ajzen, I(1991), “The Theory of Planned Behavior,” Organizational Behavior and Human Decision Processes, Vol. 50, No. 2, pp.179-211.
- [4] Fishbein M. and Ajzen(1975), “I, Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research,” Addition-Wesley, Reading, Ma.
- [5] 허윤주·이기종 (2016). 문화자본이 문화예술관광 태도 및 행동의도에 미치는 영향. 관광레저연구, 28(6), 139-157.
- [6] Armitage, C. J. & Conner, M.(2001). Efficacy of the theory of planned behaviour: Ameta-analytic review. British Journal of Social Psychology, 40(4), 471-49.
- [7] 이후석·오민재 (2016). 확장된 계획행동이론을 적용한 부산국제영화제 방문객의 행동의도 분석. 관광연구저널, 30(8), 91-104.
- [8] B. Bulgurcu, H. Cavusoglu and I. Benbasat, “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness”, MIS Quarterly, Vol. 34, No. 3, pp. 523-548, 2010.

- [9] R. West, "The Psychology of Security", *Communications of the ACM*, Vol. 51, No. 4, pp. 34-40, 2008.
- [10] M. Fishbein and I. Ajzen, *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley Publishing Company, 1975.
- [11] T. Herath and H. R. Rao, "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", *Decision Support Systems*, Vol. 47, No. 2, pp.154-165, 2009.
- [12] M. Siponen, S. Pahlila and M. A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation", *Computer*, Vol. 43, No. 2, pp. 64-71, 2010.
- [13] R. Von Solms, "Information Security Management: Why Standards are Important", *Information Management & Computer Security*, Vol. 7, No. 1, pp. 50-58, 1999.
- [14] 김도형 (2021). "금융회사를 위한 기업 정보보호 포털(EISP) 시스템의 설계 및 구현". 한국융합보안학회 융합보안논문지, Vol.21 no.1(2021). pp.101-106.
- [15] S. Lee, S. Lee and S. Yoo, "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories", *Information & Management*, Vol. 41, No. 6, pp. 707-718, 2004.
- [16] C. T. Upfold and D. A. Sewry, "An Investigation of Information Security in Small and Medium Enterprises (SMEs) in the Eastern Cape", In: H. S. Venter, J. H. P. Eloff, L. Labuschagne, & M. M. Eloff (Eds.), *Proceedings of the ISSA 2005 new knowledge today conference*, 29 June - 1 July 2005, South Africa, Article 082, pp.1 - 17, 2005.
- [17] Kim, Su Hyun (2013), A Research on Information Security Policy Compliance Activity's Effect on Stress: Centered on Compliance Activity Type p.2.
- [18] http://www.zdnet.co.kr/news/news_view.asp?article_id=201411271233339&type=det&re=zdnet_korea_article, KISA (SNC 2015) Jung, Kyoung-Ho, (2014.11.27.).
- [19] Sung Min Ryu (2013), Study on information security stress in Public Enterprise (K공사 사례를 중심으로).
- [20] 임광수 (2016), "통제수용자에 의해 인지된 정보보안정책 특성요인이 보안스트레스와 보안준수의도에 미치는 영향", 고려대 석사학위논문.
- [21] Jeong-Ha Lee (2015). A Study on the Factors for Violation of Information Security Policy in Financial Companies : Moderating Effects of Perceived Customer Information Sensitivity. *Journal of Information Technology Applications & Management*, 22(4), 225-251.
- [22] 신혜원 (2012). 기업 내 정보유출방지를 위한 내부자 위험도 분석 방법론 연구. *한국정보과학회 학술발표논문집*, 39(1C), 295-297.
- [23] 박의천, 전기석 (2021). "軍조직구성원의 보안 환경 영향요인이 보안 스트레스와 보안준수 행동에 미치는 영향 연구". 한국융합보안학회 융합보안논문지, Vol.21 no.3(2021). pp.93-104.
- [24] 정혜인 (2016), "조직구성원들의 정보보안 행동에 미치는 영향: 보호동기이론(PMT)과 계획된 행동이론(TPB) 통합을 중심으로" 남서울대학교 석사 학위논문.
- [25] Bulgurcu, B., Cavusoglu, H., and Benbasat, I(2010), "Information Security Policy Compliance : An Empirical Study of Rationality-based Beliefs and Information Security Awareness," *MIS Quarterly*, Vol. 34, No. 3, pp. 523-548.
- [26] Bulgurcu B. H and Cavusiglu, H(2009), "Roles of Information Security Awreness and Perceived Fairness in information Security Policy Compliance," *AMCIS 2009 Proceeding*, p. 419.
- [27] 홍세희 (2000), "구조방정식 모형의 적합도 지

수 선정기준과 그 근거”. 한국심리학회. <한국심리학회지 : 임상> 제19권 제1호.

[저 자 소 개]



이 광 호 (Kwang-ho Lee)
2007년 3월 육군3사관학교 국방경제학 학사
2016년 3월 연세대학교 정보보호 석사
2019년 3월 아주대학교 NCW공학 박사 수료
email : loveney@naver.com



정 찬 기 (Chan-gi Jung)
1986년 공군사관학교 전자공학 학사
1994년 플로리다공대 전산공학 석사
2001년 플로리다공대 전산공학 박사
2016년 9월 ~ 현재
아주대학교 국방디지털융합학과 교수
email : ckjeong@ajou.ac.kr