https://doi.org/10.33778/kcsa.2022.22.3.057

조직의 산업보안 활동이 구성원의 보안 정책 준수 의도에 미치는 영향★

이 동 환*, 박 승 욱**

요 약

최근 보안에 대한 중요성과 인식이 확대됨에 따라, 기업과 정부는 보안 관리를 위하여 지속적인 노력과 투자를 하고 있다. 그러나 조직에는 여전히 많은 보안 위협이 존재하며, 특히 내부직원에 의한 보안사고가 빈번하게 발생하고 있다. 그러므로 조직의 보안 관리를 위해서는 무엇보다 구성원이 보안 정책을 준수하는 것이 매우 중요하다. 따라서 본 연구는 조직적 측면의 산업보안 활동을 기술적 보안, 물리적 보안, 관리적 보안으로 분류하였고, 개인적 측면의 계획된 행동이론을 적용하여 보안 정책 준수 의도에 미치는 영향 관계를 규명하였다. 통계 분석을 위하여 SPSS 25와 AMOS 25를 활용하였으며, 연구결과, 기술적 보안은 주관적 규범에 정(+)의 영향, 물리적 보안은 지각된 행동통제에 정(+)의 영향, 관리적 보안은 태도에 정(+)의 영향, 태도와 지각된 행동통제는 보안 정책 준수 의도에 정(+)의 영향을 미치는 것으로 나타났다.

The Effect of Organization's Industrial Security Management on Employees' Security Policy Compliance Intention

Donghwan Lee*, Seungwook Park**

ABSTRACT

As the importance and awareness of security have recently expanded, companies and governments are making cont inuous efforts and investments for security management. However, there are still many security threats in the organiz ation, especially security incidents caused by internal staff. Therefore, it is very important for members to comply with security policies for organizational security management. Therefore, this study classified industrial security manageme nt into technical security, physical security, and managerial security, and applied the theory of planned behavior to inv estigate the impact relationship on the intention to comply with security policies. SPSS 25 and AMOS 25 were used for statistical analysis, and the study found that technical security had a positive(+) effect on subjective norms, physic al security had a positive(+) effect on perceived behavior control, and attitude and perceived behavior control had a po sitive(+) effect on security policy compliance intention.

Key words: Security management, Theory of planned behavior, Security policy, Security policy compliance intention, Information security, Industrial security

접수일(2022년 05월 26일), 게재확정일(2022년 09월 20일)

★ 이 논문은 2022년도 인하대학교 교내연구비 지원으로 수행된 연구임.

* 인하대학교 산업보안거버넌스 경영공학 석사(주저자)

** 인하대학교 경영학과 교수(교신저자)

1. 서론

4차 산업혁명 시대를 맞아 첨단 정보통신기술이 개발되고 발전하면서, 조직 경영에 정보 관리는 더욱 중요해졌다. 보안에 대한 중요성과 인식이 확대됨에 따라 기업과 정부는 기술 및 영업비밀 유출 방지 등 보안 관리를 위한 많은 노력과 지속적인 투자를 하고 있다. 그러나 국가정보원에 따르면, 2016년부터 5년 6개월 동안 적발한 해외 기술 유출 사건은 총 112건에 달하였으며, 예상 피해 규모는 21조 4,474억 원에 달하였다[1]. 이처럼 조직의 보안 관리에도 여전히 많은 보안 위협이 존재하고, 특히 내부적 요인으로 인한 보안사고가 지속적으로 발생하고 있다. 산업통상자원중소벤처기업위원회가 2017년부터 5년간 산업기술 및 영업비밀 유출현황을 분석한 결과, 총 유출 건수는 527건에 달하였으며, 유출 형태는 내부자 유출이 375건(71%), 외부자 유출이 152건(28.8%)로 나타났다[2]. 정병일(2009)은 대부분의 기술유출 주체가 해당 기업의 전·현직 임직원이라고 하였고[3], Bulgurcu et al.(2010) 또한 정보보안사고는 외부요인보다 내부요인에 따른 발생 빈도가 높게 나타나며, 내부위협이 조직에게 더욱 치명적이라고 하였다[4]. 이처럼 내부직원에 의한 보안 문제가 자주 발생함에 따라, 보안 관리 관점에서 내부인력 관리의 필요성이 제기되고 있다[5]. Siponen et al.(2010)은 조직에서 내부직원의 보안 정책 준수 행동을 유도할 장치가 마련되면, 내부자에 의한 보안사고를 어느 정도 예방할 수 있다고 하였다[6]. 그러나 강압적인 보안 관리와 통제는 조직의 의도와는 반대로 직원의 보안 정책 준수 의도를 감소시킬 수 있다. 따라서 조직의 보안 수준을 높이기 위해서는 내부 직원의 자발적인 보안 정책 준수 의도가 필요하다[7]. 이에 보안 전문가들은 조직에서 기술적 보안, 물리적 보안과 더불어 보안인식 교육과 같은 관리적 보안을 통하여 조직 구성원의 보안 행동 수준을 제고하도록 권고하고 있다[8]. 따라서 산업보안 활동을 다차원적으로 접근하여 보안 정책 준수 의도와의 관련성을 분석하는 연구가 필요하다. 또한 조직의 보안 관리 활동에 대하여 실제적으로 보안 행동을 통제하고 수행하는 주체는 개인이기 때문에, 자신의 태도와 환경을 고려하여 생성된 의도에 따라 행동한다는 계획된 행동이론을 활용하고자 한다. 따라서 본 연구는 조직적 측면의 산업보안 활동이 개인적 측면의 계획된 행동에 어떠한 영향을 미치는지, 그리고 계획된 행동이 보안 정책 준수 의도에 어떠한 영향을 미치는지 분석하고자 한다. 또한 연구를 통해 보안 정책 준수 의도 제고 방안을 마련함으로써, 조직의 보안 목표 달성을 위한 산업보안 활동 방향을 제시하고자 한다.

2. 이론적 배경

2.1 산업보안 활동

산업보안은 산업과 보안이 합쳐진 용어로, 범죄로부터 모든 경제활동을 보호하는 일체의 노력으로서 자산을 지키는 자산보호와 피해를 막는 손실방지, 산업자산의 안정성을 유지하는 모든 활동이나 상황 등으로 정의되고 있다[9]. 정성배(2015)는 산업보안 활동을 개인, 기업, 국가의 정보 시스템 자산을 절도·파괴·화재 등과 같은 물리적 위협으로부터 보호하는 활동과 정보의 검색·수집·저장·가공·송신·수신 도중 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 보호 활동이 융합한 것으로 보았다[10]. 김경규 외 연구진(2009)은 정보보호활동을 통제활동(물리적, 기술적, 운용적)과 관리활동(정보보호 아키텍처 구성, 정보자산 분류 및 식별, 위험분석 및 관리, 구성원 인식 및 교육)으로 분류하였으며[11], 손태현(2015)은 기술적 통제, 물리적 통제, 관리적 통제로 구분하였다[12]. 따라서 본 연구에서는 조직의 산업보안 활동을 기술적 보안, 물리적 보안, 관리적 보안으로 분류하였다.

2.1.1 기술적 보안

기술적 보안이란 정보보호 기술 및 시스템 등의 기술적 솔루션을 이용하여 정보를 관리하는 활동이며, 기업이 소유하거나 구현하려는 시스템, 네트워크, 서버, 데이터베이스 및 단말기에 따라 기술적으로 활용 가능한 보안방안을 의미한다[13][14]. 이에 네트워크 접근 통제, 시스템 개발 및 유지보수, 시스템 접근 통제, 방화벽, 외부 해킹 차단, 침입 방지 시스템, 침입 탐지 시스템, 백신, 정보기기 관리, 메일보안, 데이터 백업 등이 포함된다[14][15][16].

2.1.2 물리적 보안

물리적 보안이란 정보를 처리하는 컴퓨터, 통신기기 등과 같은 시설 및 장비들, 또는 이러한 시설이나 장비로 처리된 자료·정보를 보관하는 매체나 장소를 다양한 위협으로부터 보호하는 활동을 의미한다[17]. 이에 물리적 보호장치, 물리적 보안시스템 등과 같은 물리적 수단과 출입통제, 보안 구역 지정, 기타 장치의 보존 및 관리, 감시 및 감지, CCTV 설치, 순찰, 사고대응 등이 포함된다[13][15][16].

2.1.3 관리적 보안

관리적 보안이란 정보시스템과 연관된 인원, 조직, 기술상에 대한 전반적이고 총체적인 운영 및 유지에 관련된 보안을 의미한다[17]. 이에 보안 정책 수립, 보안 전담 조직 구성, 보안교육 프로그램, 정보보호 최고 책임자 지정 및 책임 할당, 중요자산의 식별과 분류, 직원의 채용·고용·퇴사 관리, 보안감사, 주기적 점검 등이 포함된다[15][16].

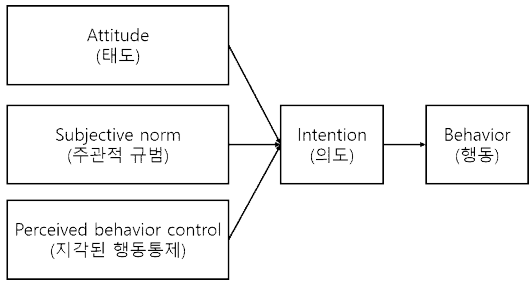
2.2 보안 정책 준수 의도

보안 정책이란 보안을 위한 기대사항을 구체적이고, 명확하며, 측정 가능한 목표와 의무조항을 포함한 기술서로, 조직 구성원이 제시된 조직의 보안 요구사항에 따라 행동하도록 하는 것을 목적으로 한다[18].

이에 보안 정책 준수 의도는 조직 구성원이 조직 내외의 잠재적인 보안 위협으로부터 조직의 자산과 정보를 보호하기 위해 규정된 보안 정책을 지키려는 의지 및 신념과 보안 정책 준수 행동에 대한 생각의 정도로 정의된다[4][6].

2.3 계획된 행동이론

Ajzen(1991)의 계획된 행동이론은 합리적 행위이론에서 발전된 이론으로, 개인의 행동을 결정하는 선행요인은 행동에 대한 의도이며, 의도는 태도, 주관적 규범, 지각된 행동통제로 구성된다[19]. (그림 1)은 계획된 행동이론의 구성요소를 도식화한 것이다.



(그림 1) 계획된 행동이론 모형

태도는 특정 행동에 대한 개인의 긍정적이거나 부정적인 감정을 의미하며, 특정한 방식으로 사람, 사물, 사건, 장소, 아이디어와 행동 등을 평가하는 개인의 인지된 경향이다[20]. 이때 평가가 바뀌면 태도가 변하며, 결과적으로 행동도 변하게 된다.

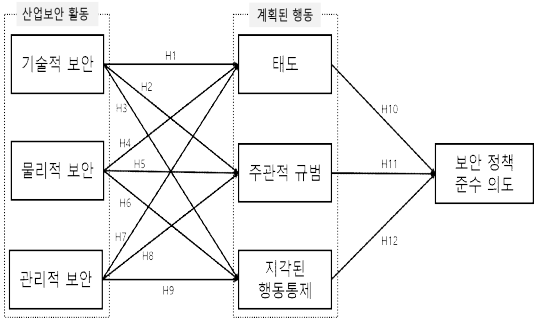
주관적 규범은 개인이 어떤 행동을 수행할 때, 친구나 동료 등 주변인들이 그 행동에 대하여 어떻게 생각할지를 의미한다. 개인의 행동에 있어 다른 사람들이 호의적으로 생각할 것 같으면 행동 의도가 높아지고, 비우호적이거나 부정적으로 생각할 것 같으면 행동 의도가 줄어든다.

지각된 행동통제는 개인이 특정 행동 실천에 대해 쉽거나 어려움의 정도를 판단하는 것을 의미하며, 행동에 필요한 기술, 능력, 기회, 자원 등을 얼마나 보유하고 있는가에 대한 정도를 의미한다[21]. 이에 개인이 자원이나 기회를 충분히 가지고 있고, 행동에 장애가 없을 것으로 생각할수록 지각된 행동통제 수준은 증가한다[19]. 지각된 행동통제는 Bandura(1977)의 자기효능감 개념과 매우 유사하기에[22], 본 연구에서 동일한 개념으로 정의하였다.

3. 연구방법

3.1 계획된 행동이론

본 연구는 조직의 산업보안 활동이 개인의 계획된 행동에 미치는 영향과 계획된 행동이 보안 정책 준수 의도에 미치는 영향을 분석하기 위하여, 다음의 (그림 2)와 같이 연구모형을 설계하였다.



(그림 2) 연구모형

3.2 연구가설

3.2.1 기술적 보안과 계획된 행동

박준경(2008)은 기업 정보보호 활동을 위한 조직 구성원의 태도와 주요 영향 요인을 분석하는 연구에서, 네트워크 보안, 방화벽 설치, 데이터 백업, 바이러스 통제, 백신, 보안 소프트웨어, 접근 통제 소프트웨어 등을 포함한 기술적 보안 시스템이 조직 구성원의 보안 태도에 영향을 미칠 것이라고 예상하였다[23]. 정우진과 이상용(2011)은 기업 정보보호 활동 중 정보에 대한 접근 권한 설정과 같은 기술적 보안이 주관적 규범과 지각된 행동통제에 영향을 미치며, 이는 내부 직원의 보안 행동 의도로 이어진다고 하였다[24]. Zhang et al.(2009)은 계획된 행동이론을 이용하여 기술적 보호가 보안 행동 의도에 영향을 미치는 요인에 대하여 연구하였으며, 데이터 백업, 파일 및 이메일 바이러스 검사, 데이터 암호화 등의 기술적 보안은 지각된 행동통제에 영향 요인임을 검증하였다[25]. 따라서 다음과 같은 가설을 설정하였다.

가설1: 기술적 보안은 태도에 정(+)의 영향을 미칠 것이다.
가설2: 기술적 보안은 주관적 규범에 정(+)의 영향을 미칠 것이다.
가설3: 기술적 보안은 지각된 행동통제에 정(+)의 영향을 미칠 것이다.

3.2.2 물리적 보안과 계획된 행동

D'Arcy & Lowry(2019)는 조직 구성원의 정보보안 정책 준수에 영향을 미치는 요인 연구에서, 직원의 네트워크 및 인터넷 사용을 추적하고 보안 감사를 수행하는 컴퓨터 모니터링 활동은 조직 구성원의 보안 정책 준수 태도에 영향을 미친다고 하였다[26]. 박준경(2008)은 기업 정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인을 분석하는 연구에서 출입 통제 시스템, 이동식 디스크 관리, 컴퓨터 암호화 통제, 조직 구성원의 인증 등을 포함한 물리적 보안 시스템이 조직 구성원의 보안태도에 영향을 미칠 것이라고 예상하였다[23]. 정우진과 이상용(2011)은 정보보호 활동에 대한 조직의 전반적인 감시자 및 감시시스템들의 감시활동이 조직 구성원의 주관적 규범에 영향을 미칠 것으로 예상하였다[24]. Zhang et al.(2009)은 물리적 보안 보호의 존재와 효과는 지각된 행동통제에 영향 요인임을 검증하였다[25]. 따라서 다음과 같은 가설을 설정하였다.

가설4: 물리적 보안은 태도에 정(+)의 영향을 미칠 것이다.
가설5: 물리적 보안은 주관적 규범에 정(+)의 영향을 미칠 것이다.
가설6: 물리적 보안은 지각된 행동통제에 정(+)의 영향을 미칠 것이다.

3.2.3 관리적 보안과 계획된 행동

Dowland et al.(1999)은 각종 정보보안 프로그램과 활동을 통해 직원에게 정보보호절차가 필요한 이유, 배경, 중요성 등을 이해시킴으로써 직원의 태도를 변화시켜야 한다고 하였으며[27], Wilson & Hash(2003)는 기업에서 실시하는 보안 교육은 직원의 보안 인식 제고와 보안에 대한 태도에 긍정적인 영향을 미친다고 하였다[28]. 박철주와 임명성(2012)은 지속적인 정보보안 정책 준수 행위 유도 요인 탐색 연구에서, 보안 정책의 포괄성과 간결성이 보안 정책 준수 태도에 유의한 영향을 미치는 것을 확인하였다[29]. Safa et al.(2015)은 정보보안 정책에 의한 경영진의 의식적이고 주의 깊은 관리 행동은 조직원 개개인의 주관적 규범에 영향을 준다고 하였다[20]. 본 연구에서는 앞서 언급한

것과 같이 지각된 행동통제와 자기효능감을 동일한 개념으로 정의하였으며, 이와 관련하여 황인호와 이혜영(2016)은 보안 정책의 목표 난이도, 구체성, 제재의 명확성이 자기효능감에 긍정적인 영향을 미친다고 하였고[30], Chen et al.(2018)은 보안 정책위반에 따른 처벌 및 해고 등의 관리적 보안 활동이 자기효능감을 매개하여 보안 정책 준수 의도에 영향을 미친다고 하였다[31]. 따라서 다음과 같은 가설을 설정하였다.

가설7: 관리적 보안은 태도에 정(+)의 영향을 미칠 것이다.
가설8: 관리적 보안은 주관적 규범에 정(+)의 영향을 미칠 것이다.
가설9: 관리적 보안은 지각된 행동통제에 정(+)의 영향을 미칠 것이다.

3.2.4 계획된 행동과 보안 정책 준수 의도

박선영(2011), 박철주와 임명성(2012)은 조직원이 보안 정책에 대한 태도가 긍정적이면 조직원은 적극적인 보안 정책 준수 의도를 갖는다고 하였다[22][29]. Herath & Rao(2009)는 정보보안 정책 준수에 관한 조직 구성원의 태도가 적극적이고 긍정적이면 조직의 보안 관련 가이드라인, 규칙, 요구사항 준수에 우호적이라고 하였고, 주관적 규범과 자기효능감 또한 정보보안 정책 준수 의도에 긍정적인 영향을 미친다고 하였다[32]. Hu et al.(2012)와 Ifinedo(2014)는 계획된 행동의 모든 요인인 태도, 주관적 규범, 지각된 행동통제가 보안 정책 준수 의도에 영향을 미친다는 것을 확인하였다[33][34]. 따라서 다음과 같은 가설을 설정하였다.

가설10: 태도는 보안 정책 준수 의도에 정(+)의 영향을 미칠 것이다.
가설11: 주관적 규범은 보안 정책 준수 의도에 정(+)의 영향을 미칠 것이다.
가설12: 지각된 행동통제는 보안 정책 준수 의도에 정(+)의 영향을 미칠 것이다.

3.3 변수의 조작적 정의

본 연구는 선행연구와 이론에서 신뢰성과 타당성이 검증된 개념을 참조하였으며, 연구 목적에 맞게 일부 수정하였다. 변수의 조작적 정의는 다음의 <표 1>과 같으며, 모든 문항은 Likert 5점 척도로 측정하였다.

<표 1> 변수의 조작적 정의

변수	조작적 정의	참고문헌
기술적 보안	조직의 정보 유출 방지를 위한 정보기술 관리 활동	[10] [14] [35]
물리적 보안	조직의 정보 유출 방지를 위한 중요시설 관리 활동	[10] [35]
관리적 보안	조직의 정보 유출 방지를 위한 정책 및 운영 관리 활동	[10] [35]
태도	보안 정책 준수에 대한 개인의 긍정적 또는 부정적 판단 및 인식	[19] [20] [36]
주관적 규범	보안 정책 준수에 대한 주변의 사회적 압력에 대한 개인의 인식	[19] [20] [36]
지각된 행동통제	보안 정책 준수 행동을 얼마나 잘 수행하고 통제할 수 있는지에 대한 개인의 평가	[19] [20] [32] [36]
보안 정책 준수 의도	보안 정책 준수를 위하여 실제적인 행동을 실행 또는 실천하고자 하는 의향	[19] [29] [32] [36]

3.4 자료수집 및 분석 방법

본 연구는 2022년 4월 5일부터 2022년 4월 13일까지 직장인을 대상으로 온라인 설문을 진행하였으며, 총 310건의 자료를 수집하였다. 데이터클리닝 과정을 통해 불성실하게 응답한 4건을 제외하여, 총 306건의 자료를 최종 표본으로 선정하였다. 통계 분석을 위한 도구로는 SPSS 25와 AMOS 25를 활용하였다.

4. 연구결과

4.1 인구통계학적 특성 분석

본 연구의 최종 분석 대상은 기업 및 기관 등의 조직에서 근무하는 인원 306명으로, 표본의 인구통계학적 특성은 다음 <표 2>와 같다.

<표 2> 응답자 인구통계학적 특성

구분		빈도 (명)	비율(%)
성별	남	164	53.6
	여	142	46.4
연령	20대	14	4.6
	30대	89	29.1
	40대	116	37.9
	50대 이상	87	28.4
학력	고졸 이하	40	13.1
	전문학사	39	12.7
	학사	204	66.7
	석사	23	7.5
조직 형태	스타트업 및 벤처기업	17	5.6
	중소기업	130	42.5
	중견기업	78	25.5
	대기업	51	16.7
	연구기관	6	2.0
	공공기관	22	7.2
	기타	2	0.7

4.2 측정도구 분석

4.2.1 개념타당성 검정

개념타당성 검정을 위해 SPSS 25를 활용하여 탐색적 요인분석을 실시하였다. 탐색적 요인분석에서 요인적재량은 변수들의 중요도를 나타내고, 고유값이 1.0 이상, 요인적재량이 0.4이상이면 유의한 변수로 간주하며, 0.5이상이면 아주 중요한 변수로 본다[37].

요인 추출 방법은 주성분 분석을 사용하였으며, 회전 방법은 카이저 정규화가 있는 베리멕스를 사용하였다. 탐색적 요인분석 결과는 <표 3>과 같으며, 결과에 따라 기술적 보안의 측정항목 1개(기술2), 물리적 보안의 측정항목 1개(물리7), 관리적 보안의 측정항목 1개(관리2), 태도의 측정항목 1개(태도5)가 제외되었다. 전체 41개의 항목 중 4개를 제외한 항목들에 대하여 고유값 1.0 이상, 요인 적재량 0.50 이상, 변수별로 항목들이 잘 묶이는 것으로 나타났기에, 구성 개념들을 측정하는 각각의 항목들이 해당 개념을 적절하게 측정하고 있음이 입증되었다.

<표 3> 탐색적 요인분석 결과

항목	공통성	요인						
		1	2	3	4	5	6	7
기술6	.701	.809	.098	.134	.113	.062	.045	-.004
기술8	.698	.798	.163	.072	.164	.006	.049	.018
기술3	.658	.782	.082	.112	.129	.037	.065	.067
기술7	.633	.776	.028	.121	.112	-.030	.025	.029
기술4	.634	.765	.128	.065	.160	.040	.017	.025
기술1	.651	.740	.240	.130	.123	.036	.106	.035
기술5	.546	.695	.062	.157	.079	.096	.039	.132
관리7	.619	.038	.768	.054	.108	-.004	.055	.106
관리5	.616	.104	.753	.034	.181	-.024	-.049	.039
관리4	.624	.158	.745	-.066	.191	-.021	.009	.052
관리1	.565	.147	.716	-.009	.115	.085	.023	.105
관리8	.547	.137	.711	-.041	.117	.020	.049	.070
관리6	.545	-.034	.694	.055	.124	-.055	.037	.199
관리3	.519	.191	.670	-.046	.129	.118	.024	-.011
규범2	.810	.141	.041	.878	.079	.069	.034	.070
규범4	.787	.159	-.019	.863	.010	.072	-.002	.105
규범5	.750	.134	-.011	.849	.026	.103	-.011	.003
규범1	.776	.201	.004	.843	.106	.058	.034	.094
규범3	.709	.094	-.032	.828	.032	.062	-.080	.038
물리4	.615	.082	.129	.088	.758	.036	.048	.069
물리3	.591	.078	.116	-.001	.751	.068	.025	.046
물리6	.634	.279	.165	.032	.718	.109	.020	.014
물리5	.542	.160	.111	.072	.703	.001	.034	.058
물리1	.569	.072	.238	.084	.695	.072	.097	-.055
물리2	.549	.187	.202	-.021	.687	.010	.004	.016
통제3	.728	.004	.014	.093	.005	.840	.115	.019
통제2	.718	.104	.016	.054	.118	.818	.137	.046
통제4	.664	.051	.055	.033	.132	.793	-.082	.070
통제1	.641	.033	.007	.148	-.004	.776	.113	.058
의도4	.730	.045	.021	-.049	.050	.028	.846	.079
의도3	.662	.049	-.007	.000	.009	.077	.808	.032
의도2	.635	.085	.012	.056	.078	.013	.783	.072
의도1	.622	.080	.099	-.041	.052	.152	.757	.070
태도3	.699	.046	.065	.130	.064	.075	-.035	.815
태도4	.646	.086	.099	.075	.014	.024	.075	.785
태도2	.645	.029	.084	.075	.016	.080	.127	.780
태도1	.623	.076	.237	-.014	.040	.012	.095	.741

note: KMO=0.859, Bartlett's=5866.670 ($p<0.001$)

4.2.2 신뢰성 검정

신뢰성을 분석할 때, 크론바흐 알파값이 0.6~0.7이면 활용가능한 수준이고, 0.7~0.9이면 적절하고, 그 이상이면 우수하다고 판단한다[38].

신뢰성 검정 결과는 다음의 <표 4>와 같으며, 기술적 보안과 주관적 규범의 크론바흐 알파값은 0.90 이상, 물리적 보안, 관리적 보안, 태도, 지각된 행동통제, 보안 정책 준수 의도의 크론바흐 알파값은 0.80 이상으로, 측정 개념 모두 신뢰수준을 만족하는 것으로 나타났다.

<표 4> 신뢰성 검정 결과

측정 개념	신뢰도 (Cronbach' α)
기술적 보안	.905
물리적 보안	.844
관리적 보안	.868
태도	.815
주관적 규범	.921
지각된 행동통제	.839
보안 정책 준수 의도	.826

4.2.3 집중타당성 검정

집중타당성 검정을 위해 AMOS 25를 활용하여 확인적 요인분석을 실시하였다. 척도의 타당성과 신뢰성이 있으려면 표준화 요인적재량이 0.5 이상이고, 지표의 내적 일관성을 측정한 개념신뢰도가 0.7 이상이면서, 개념에 대하여 지표가 설명할 수 있는 분산의 크기를 나타내는 AVE(Average Variance Extracted)값이 0.5이상이어야 한다[39].

확인적 요인분석의 결과는 다음 <표 5>와 같으며, 집중타당성을 감소시키는 물리적 보안의 측정항목 2개(물리4, 물리5)와 관리적 보안의 측정항목 1개(관리3)를 제외하였다. 표준화 요인적재량은 모두 0.6 이상, 개념신뢰도는 모두 0.8 이상, AVE값은 모두 0.5 이상으로 기준치에 부합되기에, 측정항목이 구성개념을 일관성 있게 잘 측정한다는 것이 입증되었다.

<표 5> 확인적 요인분석 결과

변수	문항	C.R.	표준화계수	개념 신뢰도	AVE
기술적 보안	기술1	11.890	0.765	0.906	0.579
	기술3	11.962	0.770		
	기술4	11.686	0.750		
	기술5	—	0.672		
	기술6	12.415	0.805		
	기술7	11.649	0.747		
	기술8	12.484	0.810		
물리적 보안	물리1	—	0.707	0.803	0.506
	물리2	10.685	0.719		
	물리3	9.731	0.643		
	물리6	11.213	0.771		
관리적 보안	관리1	11.361	0.697	0.858	0.503
	관리4	12.305	0.758		
	관리5	11.619	0.714		
	관리6	10.827	0.664		
	관리7	—	0.730		
	관리8	11.203	0.688		
태도	태도1	10.690	0.708	0.816	0.526
	태도2	—	0.720		
	태도3	11.167	0.751		
	태도4	10.844	0.721		
주관적 규범	규범1	17.858	0.852	0.922	0.703
	규범2	18.660	0.877		
	규범3	15.530	0.774		
	규범4	18.196	0.862		
	규범5	—	0.825		
지각된 행동통제	통제1	11.096	0.713	0.840	0.568
	통제2	12.126	0.797		
	통제3	12.024	0.787		
	통제4	—	0.714		
보안정책 준수의도	의도1	—	0.692	0.828	0.547
	의도2	10.584	0.707		
	의도3	10.919	0.735		
	의도4	11.648	0.817		

*** P<0.001

4.2.4 판별타당성 검정

판별타당성은 서로 다른 잠재변수 간의 차이를 나타내는 정도로서, 잠재변수 간 낮은 상관을 갖는다면 판별타당성이 있는 것을 의미한다(우종필, 2012). 이에 AVE 제곱근값이 0.7 이상이고, AVE 제곱근값이 다른 변수의 상관계수값보다 높을 때, 판별타당성이 있다고 판단할 수 있다[40].

<표 6>에서 대각선 방향으로 별표(*) 표시한 값은 AVE 제곱근값이며, 나머지 행렬의 값은 각 변수의 상관계수값이다. 판별타당성 검정 결과, AVE 제곱근값이 각 변수의 상관계수값보다 높으며, 모두 0.7 이상의 값으로 나타나 판별타당성을 확보하였다.

<표 6> 판별타당성 검정 결과

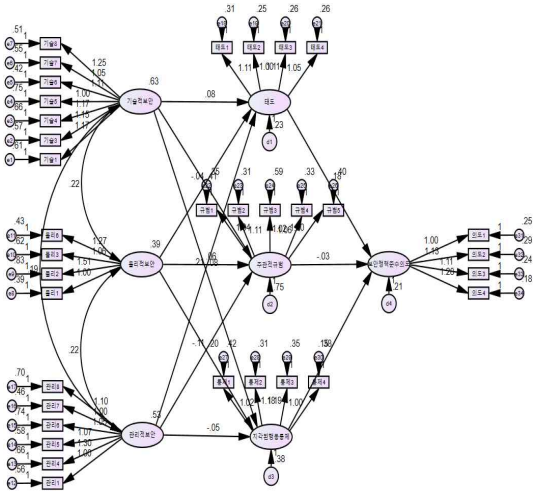
변수	기술적 보안	물리적 보안	관리적 보안	태도	주관적 규범	지각된 행동통제	보안정책 준수의도
기술적 보안	**0.761***						
물리적 보안	0.450	**0.711***					
관리적 보안	0.339	0.485	**0.709***				
태도	0.188	0.142	0.321	**0.725***			
주관적 규범	0.341	0.152	0.048	0.207	**0.839***		
지각된 행동통제	0.157	0.209	0.069	0.168	0.220	**0.754***	
보안정책 준수의도	0.173	0.145	0.105	0.202	0.017	0.215	**0.739***

*AVE 제곱근값

4.3 구조방정식 모형 분석

4.3.1 구조방정식 모형의 적합도 검정

본 연구는 AMOS 25를 이용하여 (그림 3)과 같이 구조방정식 모형을 설계하였다. 구조방정식 모형에는 7개의 잠재변수와 34개의 관측변수가 포함되었다.



(그림 3) 구조방정식 모형

구조방정식 모형의 적합도 검정 결과, 기준치에 모두 부합되어 모형의 적합도는 전반적으로 우수하다고 판단된다. 구조방정식 모형의 적합도 검정 결과는 다음의 <표 7>과 같다.

<표 7> 구조방정식 모형의 적합도 검정 결과

적합도 지수			지표 값	임계치 기준
절대적합지수	모형 전반 적합도	χ^2(CMIN)	771.949 (P<0.001)	p≦0.05~0.10
		χ^2(CMIN)/DF	1.508	1.0≦CMIN/df ≦2.0~3.0
		RMSEA	0.041	≦0.05~0.08
		RMR	0.057	≦0.08
	모형 설명력	GFI	0.871	≧0.8~0.9
		AGFI	0.850	≧0.8~0.9
증분적합지수		NFI	0.861	≧0.8~0.9
		TLI	0.943	≧0.8~0.9
		CFI	0.948	≧0.8~0.9
간명적합지수		PNFI	0.786	≧0.6
		PCFI	0.865	≧0.5~0.6
		PGFI	0.749	≧0.5~0.6

4.3.2 가설 검증

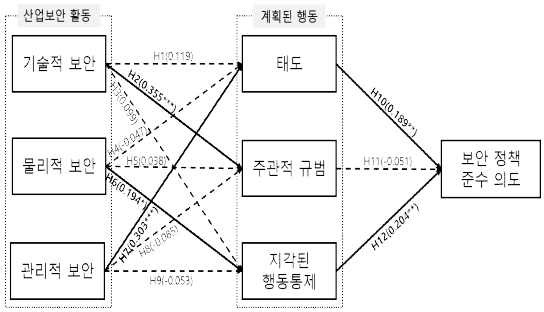
연구모형 가설의 검증을 위하여 AMOS 25를 사용하여 각각의 변수 간 설정된 인과관계에 대한 경로분석을 실시하였다. 연구모형 가설 검증 결과는 다음의 <표 8>과 같다.

<표 8> 연구모형 가설 검증 결과

가설	가설경로			경로 계수	C.R.(t)	p-value	검증 결과
H1	기술적 보안	→	태도	0.119	1.577	0.115	기각
H2	**기술적 보안**	**→**	**주관적 규범**	**0.355**	**4.787**	***	**채택**
H3	기술적 보안	→	지각된 행동통제	0.099	1.317	0.188	기각
H4	물리적 보안	→	태도	-0.047	-0.540	0.589	기각
H5	물리적 보안	→	주관적 규범	0.038	0.473	0.636	기각
H6	**물리적 보안**	**→**	**지각된 행동통제**	**0.194**	**2.168**	**0.030***	**채택**
H7	**관리적 보안**	**→**	**태도**	**0.303**	**3.654**	***	**채택**
H8	관리적 보안	→	주관적 규범	-0.085	-1.158	0.247	기각
H9	관리적 보안	→	지각된 행동통제	-0.053	-0.665	0.506	기각
H10	**태도**	**→**	**보안정책 준수의도**	**0.189**	**2.720**	**0.007****	**채택**
H11	주관적 규범	→	보안정책 준수의도	-0.051	-0.809	0.418	기각
H12	**지각된 행동통제**	**→**	**보안정책 준수의도**	**0.204**	**2.966**	**0.003****	**채택**

* P<0.05, * P<0.01, *** P<0.001

가설 검증 결과, 가설2, 가설6, 가설7, 가설10, 가설12가 채택되었다. 기술적 보안은 주관적 규범에 영향을 미치고, 태도와 지각된 행동통제에는 영향을 미치지 않는 것으로 나타났다. 물리적 보안은 지각된 행동통제에 영향을 미치고, 태도와 주관적 규범에는 영향을 미치지 않는 것으로 나타났다. 관리적 보안은 태도에 영향을 미치고, 주관적 규범과 지각된 행동통제에는 영향을 미치지 않는 것으로 나타났다. 주관적 규범을 제외한, 태도와 지각된 행동통제는 보안 정책 준수의도에 영향을 미치는 것으로 나타났다. 가설 검증 결과를 요약하면 다음의 (그림 4)와 같다.



(그림 4) 가설 검증 결과 요약

5. 결론

본 연구는 실증분석을 통해, 조직 구성원의 보안 정책 준수 의도에 대한 조직적 측면의 산업보안 활동과 개인적 측면의 계획된 행동의 영향 관계를 규명하였다.

본 연구의 학문적 시사점은 다음과 같다. 첫째, 기존 연구에서는 주로 보안 활동 중 단일 영역에서 연구를 진행하였지만, 본 연구는 산업보안 활동을 세 가지 영역으로 구분하고 통합적으로 분석하였다. 둘째, 기존 연구에서 사용한 산업보안 활동을 보다 넓은 항목으로 측정하였고, 타당성과 신뢰성을 검증하여 기술적·물리적·관리적 보안의 개념을 재정의하였다. 셋째, 기존 연구 중 계획된 행동이론의 변수 일부만을 사용하는 경우가 다수 존재하였는데, 본 연구에서는 계획된 행동이론 모형을 그대로 활용하여 실증적으로 분석하였다.

다음으로 본 연구의 실무적 시사점은 다음과 같다. 첫째, 물리적 보안은 지각된 행동통제에 영향을 미치고, 지각된 행동통제는 보안 정책 준수 의도에 영향을 미치는 것으로 확인되었기 때문에, 출입통제, 순찰·경비 활동, 영상감지, 보호구역의 설정 등 물리적 보안을 더욱 적극적으로 시행하여야 한다. 보안에 대한 가시성과 영역성을 충분히 노출하는 물리적 보안 활동을 통해, 조직원들에게 보안 정책을 어려움 없이 준수할 수 있다는 자신감과 믿음을 줄 수 있는 분위기와 환경을 조성해야 한다. 둘째, 관리적 보안은 태도에 영향을 미치고, 태도는 보안 정책 준수 의도에 영향을 미치는 것으로 확인되었기 때문에, 조직은 보안교육 등 관리적 보안을 통해 구성원이 보안 정책 준수에 대한 긍정적인 태도를 가질 수 있게 유도해야 한다. 이를 위하여 조직 구성원에게 보안 정책 준수에 대한 중요성과 필요성을 지속적으로 인식시켜야 하는데, 획일적인 집체교육 방식으로는 그 효과를 기대하기 어려우며[40], 조직원들이 근무하는 직종에 적합한 형태의 다채로운 교육 실시와 기존 문서 중심에서 탈피하는 보안 콘텐츠의 개발이 필요하다[41]. 즉, 보안교육이 일방적인 강의식 교육보다 교육 대상자의 직접적인 참여를 유도하고 커뮤니케이션을 통하여 상호 공유할 수 있도록 실시해야 하며[42], 교육목표에 따른 보안역량 수준을 구체적으로 설정하고, 교육평가를 통해 우수직원에게 포상하여 보안교육의 효과를 높여야 한다[43]. 셋째, 조직은 효과적인 산업보안 활동을 위해서 기술적·물리적·관리적 보안의 영역 모두 유기적으로 설계하고 관리해야 하지만, 보안 설계와 관리에 부담이 있을 경우, 조직 상황에 맞게 기술적 보안은 기본적인 선까지 구축하고, 물리적 보안과 관리적 보안에 투자를 확대하는 것이 보안 관리에 더욱 유리하다. 그러나 보안사고는 다양한 요인들에 의해서 복합적으로 발생하기 때문에, 조직은 보안 관리가 특정 영역에 과도하게 편중되지 않도록 전사적 차원에서 관리해야 한다.

본 연구의 한계점은 다음과 같다. 첫째, 주관적 규범의 경우 보안 정책 준수 의도에 영향을 미치지 않는다는 연구결과가 나타나, 기존 연구와 상반된 결과를 보였다. 따라서 향후 연구에서는 정부기관, 공공기관, 대기업, 핵심 기술을 보유한 기업 등 성실하게 산업보안 활동을 하는 조직을 대상으로 계획된 행동 요인이 보안 정책 준수 의도에 미치는 영향을 재검증할 필요가 있다. 둘째, 본 연구에서는 보안 정책 준수 의도가 실제 보안 정책 준수 행동으로 연결되는지에 대한 분석은 진행하지 못하였다. 그러므로 향후 연구에서는 보안 정책 준수 의도와 보안 정책 준수 행동의 관계를 실증적으로 검증할 필요가 있다.

참고문헌

[1] 윤홍우, “국가 핵심 기술 유출만 35건…피해 규모 최소 21.4조 달해”, 서울경제, 2021, 검색일 2022년 2월 10일. https://www.sedaily.com/NewsView/22OZZFATQB.

[2] 김용언. “산업기술·영업비밀 5년간 527건 유출… 중소기업 피해 482건”, 세계일보, 2021, 검색일 2022년 2월 23일. https://segye.com/view/20210919504487.

[3] 정병일, “기업의 산업기술 유출방지 연구”, 한국산업보안연구, 제1권, 제1호, pp. 1-19, 2009.

[4] Bulgurcu, B., Cavusoglu, H., & Benbasat, I., “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness”, MIS Quarterly, Vol. 34, pp 523-548, 2010.

[5] 김현호, 강현, 최연준. “산업보안 핵심인력의 인적자

원관리가 직무태도에 미치는 영향: 관계·위계문화를 중심으로", 한국산업보안연구, 제7권, 제2호, pp. 7-31, 2017.

[6] Vance, A., Siponen, M., & Pahnila, S., "Motivating IS security compliance: Insights from habit and protection motivation theory, Information & Management", Vol. 49, Issue 3-4, pp.190-198, 2012.

[7] Guo, K. H., Yuan, Y., Archer, N. P. & Connelly, C. E., "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model", Journal of Management Information Systems, 28(2):203-236, 2011.

[8] Hovav, A. & D'Arcy, J., "Applying an Extended Model of Deterrence Across Cultures: An Investigation of information Systems Misuse in the U.S. and South Korea", Information and Management, Vol. 49, No. 2, pp. 99-110, 2012.

[9] 임창묵, "기술유출방지를 위한 정책수단에 관한 연구", 「과학수사학회지」, 6(1):1-9, 2012.

[10] 정성배, "산업보안 관리활동이 기업의 보안성과와 업무효율성에 미치는 영향", 박사학위논문, 용인대학교 대학원, 2015.

[11] 김경규, 신호경, 박성식, 김범수, "정보자산보호성과가 조직성과에 미치는 영향에 관한 연구: 관리활동과 통제활동을 중심으로", Journal of Information Science Theory and Practice, 40(3), 61-77, 2009.

[12] 손태현, "기업의 정보보호활동이 정보보안과 정보경영 성과에 미치는 영향", 「박사학위논문」, 명지대학교 대학원, 2015.

[13] 한국산업보안연구학회, '산업보안학', 박영사, 2019.

[14] Post, G., & Kagan, A., "Management tradeoffs in anti-virus strategies", Information & Management, Vol. 37, No. 1, pp. 13-24, 2000.

[15] 정구헌, 정승렬, "정보보호 통제활동이 조직유효성에 미치는 영향 : 정보활용의 조절효과를 중심으로", 지능정보연구, 17(1), 71-90, 2011.

[16] 박호진, "정보보안 테크노스트레스가 개인만족에 미치는 영향" 국내석사학위논문, 한국외국어대학교 경영대학원, 2015.

[17] 중소기업청, '보안컨설턴트용 실무 가이드북' 한국산업기술진흥협회, 2007.

[18] Goel, S., & Chengalur-Smith, I. N., "Metrics for Characterizing the Form of Security Policies", Journal of Strategic Information Systems, 19, 281-295. 2010.

[19] Ajzen, I., "The Theory of Planned Behavior", Organizational Behavior and Human Decision Processes, 50(2), 179-211, 1991.

[20] Safa N. S., Sookhak. M., Solms R. V., Furnell F., Ghani N. A., & Herawan, T., "Information security conscious care behaviour formation in organizations", Computers & Security, Volume 53, Pages 65-78, 2015.

[21] Ong, T. F., & Musa, G., "An examination of recreational divers' underwater behaviour by attitude - behaviour theories", Current Issues in Tourism, 14:8, 779-795, 2011.

[22] 박선영, "정보보안 정책 준수 의도에 대한 영향요인", 한국전자거래학회지, 16(4), 33-51, 2011.

[23] 박준경, "기업 정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인", 석사학위논문, 연세대학교 정보대학원, 디지털 비즈니스 전공, 2008.

[24] 정우진, 이상용, "금융회사의 고객정보보호에 대한 내부직원의 태도 연구", 한국경영정보학회 추계통합학술대회, pp. 670-679, 2011.

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

[26] D'Arcy, J. & Lowry, P. B., "Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study", Inf. Syst. J, 29, 43 - 69, 2019.

[27] Dowland, P. S., Furnell, S. M., Illingworth, H. M., & Leynolds, P. L., "Computer crime and abuse: a survey of public attitudes and awareness", Computers and Security, vol. 18, pp. 715-726, 1999.

[28] Wilson, M., & Hash, J., “Building an information technology security awareness and training program”, NIST Special Publication, 800(50), 1-39, 2003.

[29] 박철주, 임명성, “보안 대책이 지속적 보안 정책 준수에 미치는 영향”, 디지털정책연구, 10(4), 23-35, 2012.

[30] 황인호, 이혜영, “조직구성원의 정보보안 정책 준수의도: 계획된 행동이론, 목표설정이론, 억제이론의 적용”, 디지털융복합연구, 14(7), 155-166, 2016.

[31] Chen, X., Wu, D., Chen, L., & Teng, J. K. L., “Sanction severity and employees’ information security policy compliance: Investigating mediating, moderating, and control variables”, Information & Management, 55(8):1049-1060, 2018.

[32] Herath, T., & Rao, H. R., “Protection motivation and deterrence: A framework for security policy compliance in organisations”, European Journal of Information Systems, 18(2), pp.106-125, 2009.

[33] Hu, Q., Dinev, T., Hart, P., & Cooke, D., “Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture”, Decision SciencesVolume 43, Issue 4 p. 615-660. 2012.

[34] Ifinedo, P., “Information systems security policy compliance: An empirical study othe effects of socialization, influence, and cognition”, Information & Management, Vol. 51, No. 1, pp.69-79, 2014.

[35] 정병호, “기밀정보 유출 경험을 가진 기업들의 정보사고 대응역량 강화에 관한 연구”, 디지털산업정보학회, 12(2), 73-86, 2016.

[36] 신혁, “계획행동 요인을 매개로 경영진 역할과 보호동기가 정보보안정책 준수에 미치는 영향”, 박사학위논문, 건국대학교 대학원, 2018.

[37] 송지준, ‘논문작성에 필요한 SPSS/AMOS 통계분석방법’, 개정2판, 경기: 21세기사, 2012.

[38] Nunnally, J.C., ‘Psychometric theory’, 2nd ed., New York: McGraw-Hill, 1978.

[39] 우종필, ‘우종필 교수의 구조방정식 모델 개념과 이해’, 서울: 한나래아카데미, 2012.

[40] Fornell, C., & Larcker, D. F., “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error”, Journal of Marketing Research, 18, 382-388, 1981.

[40] 최종현, “게임을 통한 정보보안인식 향상에 관한 연구: 개별 정보보안정책에 대한 인식변화를 중심으로”, Journal of the Korea Institute of Information Security & Cryptology, 28(4), 951-962, 2018.

[41] 이치석, 김양훈, “보안교육과 보안관리 역량의 상관관계 분석: 인가된 내부자 기밀유출사례를 중심으로”, 한국전자거래학회지, 20(2), 27-36, 2015.

[42] 김형근, 안상희, “산업보안 교육훈련의 효과성 제고를 위한 교수학습 환경 설계 방안”, 한국산업보안연구, 4(2), 241-261, 2014.

[43] 엄정호, “효과적인 사이버보안 교육훈련을 위한 교육과정 문제점 및 개선 방안”, 보안공학연구논문지, 12(4), 337-350, 2015.

〔저자소개〕

이 동 환 (Donghwan Lee)
2020년 8월 인하대학교 경영학 학사
2022년 8월 인하대학교 산업보안
거버넌스 경영공학 석사
email : donghwan373@naver.com

박 승 욱 (Seungwook Park)
1985년 2월 연세대학교 경영학 학사
1991년 6월 오하이오주립대학교
경영학 석사
1999년 12월 오하이오주립대학교
경영학 박사
1999년 8월 California State Univ.
Fullerton 부교수
2007년 3월 ~ 현재
인하대학교 경영학과 교수
email : separk6112@inha.ac.kr