한국항해항만학회지 제43권 제3호
J. Navig. Port Res. Vol. 43, No. 3 : 179-185, June 2019 (ISSN:1598-5725(Print)/ISSN:2093-8470(Online))
DOI : http://dx.doi.org/10.5394/KINPR.2019.43.3.179

항만물류조직구성원들의 보안능력에 영향을 미치는 요인

† 강다연

† 경북대학교 경영학부 BK21플러스 Post-Doc

Factors Affecting the Security Ability of Port Logistics Organization Members

† *Da-Yeon Kang*

† *BK21 PLUS School of Business Administration Kyungpook National University, Daegu 41566, Korea*

요 약 : 현재 항만물류보안과 관련한 노력이 활발하게 일어나고 있지만 항만정보기술과 관련된 보안에 대해서는 인식과 교육, 제도 등이 부족한 상황이다. 상호인증 협약 수립을 통해 항만물류보안 정보를 실시간으로 교환 할 수 있는 통합 네트워크를 구축할 필요성이 있다. 항만 경쟁력 확보 및 물류 서비스 강화를 목적으로 물류보안을 위한 국가 전략수립이 중요하다. 무엇보다 시급히 필요한 것은 항만물류조직구성원들의 보안의식을 높이고 항만물류조직의 중요한 특성인 정보 보안 능력을 향상시키는 것이다. 따라서 본 연구는 항만물류조직구성원들의 정보보안능력에 영향을 미치는 요인을 분석하였다. 분석결과 보안규범이 보안인식에 영향을 미친다는 가설은 기각되었지만 보안활동과 보안인식 간의 관련성은 유의한 것으로 나타났다. 또한 보안규범과 보안능력 간의 관계, 보안인식과 보안능력 간의 관계에도 긍정적인 영향을 미치는 결과로 나타났다.

핵심용어 : 항만물류보안, 보안규범, 보안활동, 보안인식, 보안능력

Abstract : *Currently, despite having active movements related to port logistics security, there is lack of awareness, education, and security systems related to port technology. Before implementing port logistics security, a mutual authentication agreement should be reached through the establishment of an integrated network that can share port logistics security information in real time. In order to achieve port competitiveness and strengthen logistics service, establishment of national strategy for logistics security is necessary. However, there is an urgent need to raise the security consciousness among the port logistics organization members and enhance the information security ability which is a crucial feature of the port logistics organization. Therefore, the objective of this study is to analyze the factors affecting the information security capacity of port logistics organization members. Even though the analysis rejected the hypothesis that security regulations affect security awareness, the security activities and security awareness were significantly correlated. It also has a positive impact on the relationship between security norms and security abilities, and security awareness and security abilities.*

Key words : *Port Logistics Security, Security Regulation, Security Activity, Security Awareness, Security Abliity.*

1. 서 론

치열한 경쟁 환경에 처한 항만에서의 적합한 보안체계는 조직의 경쟁력 우위를 강화하기 위한 전략적인 수단이다. 오늘날의 항만은 친환경 터미널, 하역처리 능력의 상승, 컨테이너 처리작업의 고속화, 노동력의 절감을 위해 관련 항만운영 부분에서 시스템과 제도를 갖추고 있다. 세계 각국과 국제기구에서는 IMO, OECD 등의 기구를 설립하고 제도를 도입하여 선박과 항만 등 물류부문의 보안을 강화하기 위한 방안을 마련하고 있다(Ministry of Maritime Affairs and Fisheries, 2016). 국내에서도 물류보안의 중요성을 강조하고 있지만, 아직까지 항만기술과 관련된 정보보안에 대해서 조직구성원들의 인식과 교육이 부족한 상황이며, 특히 조직 내부에서 제도적으로 갖추어야 할 보안정책에 대한 이해가 부족한 실정이다.

항만물류조직의 정보보안은 정보가 유출되지 않게 관리하기 위한 전략을 구축해야하고 조직의 특성을 반영한 보안정책 사항과 보안정책 준수에 관한 규정사항에 대한 검토와 관리가 필요하다(Kang, 2013). 우선 조직내부에서 준수해야 할 보안사항을 관리하기 위해서는 기존의 조직의 보안지침과 보안교육, 보안훈련이 정기적으로 시행되어야 한다(Kim et al, 2009). 항만물류 조직의 대부분의 업무가 정보시스템을 기반으로 이루어지고 있는 상황에서 데이터관련 업무의 오류, 수정, 갱신, 삭제 등 정보시스템기반의 체계적인 통합업무가 필수적인 사항이다. 따라서 정보시스템을 통한 업무처리에 있어서 조직의 정보 유출에 대한 피해를 최소화시키기 위한 정보 보안방안을 강화하는 것이 필수적이다(Anderson and Agarwal, 2010).

조직의 중요한 정보자산의 손실을 목적으로 접근하여 기업정보를 유출시키는 경우는 조직 외부요인 보다 내부위협 요인

† Corresponding author : 정회원, kdy2019@knu.ac.kr 053)950-7330

에 의해 발생하는 빈도가 높다. 조직 내부위협으로부터 발생한 피해는 조직의 성장발전을 저해하기도 하며 사회적·경제적으로도 막대한 손실을 가져다준다. 이에 대응하기 위해 사전에 보안관리를 위한 기업의 보안 관련 가이드라인이 필수적으로 요구된다. 조직의 정보자산을 보호할 수 있는 기업내부의 구체적인 보안지침과 체계적인 정보보안정책을 기반으로 조직구성원들의 보안능력이 마련되어 있어야 기업보안 사고에 대한 피해와 이로 인한 손실을 줄일 수 있다(Kim and Song, 2011; Shim, 2011). 지금까지 항만물류분야의 정보보안 관련 연구는 주로 시스템 보안, 물리적 보안 관련 연구가 주를 이루고 있어 인적 사고와 같은 관리적 측면에서의 항만물류보안 연구는 미흡한 실정이다. 항만물류분야는 업무활동 거래에서 발생되는 정보전산과 관련되어 있는 조직의 중요한 자산을 안전하게 보안적인 차원에서 관리하는 것이 우선적으로 중요하다. 또한 기본적이면서 반드시 필요한 조직구성원들의 정보보안의 인식의 제고와 함께 실천하며 강조되어야 할 사항들에 대해 권고하는데 연구의 목적을 두고자 한다. 따라서 본 연구에서는 항만물류조직구성원들의 정보보안 능력 향상에 긍정적인 영향을 미치는 요인들을 알아보고자 한다.

2.이론적 배경

2.1 항만물류 보안 및 관련 연구

항만물류보안은 내륙지역에서 이루어지는 물류활동에 대한 보안과 국제 물류활동에 포함되는 모든 물류활동에 대한 포괄적인 보안이다(Ministry of Maritime Affairs and Fisheries, 2013). 항만물류보안제도에는 ISPS Code((The International Ship and Port Facility Security Code)제도가 있다. 이는 해상테러 대비를 위해 제정된 국제 선박 및 항만시설 보안 코드로써 국제 항해에 종사하는 선박 및 선박이 이용하는 항만 시설을 대상으로 보안 의무 및 지침을 규정하고 있다. 전 세계의 항만 시설의 크기 및 인프라가 다르고 선박의 종류마다 취해야 할 보안 조치도 다르기에 ISPS Code는 특정 조치를 강요하는 대신 선박 및 항만 시설에 대한 표준화된 프레임이 필요하다. Ko(2011)은 국제물류보안 인증제도를 분석하고 국가 공급사슬보안체계 구축의 기본방향을 글로벌 수준의 공급사슬보안체계구축, 국내적으로 효율적 운영체계구축, 국가적 차원의 지원체계 구축의 관점으로 제시하였다. Park(2007)는 물류정책의 통합과 조정기능 강화를 위한 방안으로 물류법제 개선에 대해 정부정책수립과 물류사업발전을 위한 규제완화의 필요성을 언급하였다.

물류보안체계 구축을 지원하기 위해 국제표준화기구에서 제정한 물류보안경영시스템 인증제도가 있다. 산업전반의 어느 조직에서든 적용될 수 있도록 PDCA방법론에 기초한 보안경영시스템이다. 그러나 우리나라에서의 완벽한 물류보안체제가 구축되어 있지 않은 상황이므로 물류 전 구간을 완벽히 통합하는 물류보안제도를 체계적으로 도입하는 방안을 모색하는 것이 필요하다. 해양수산부는 물류보안을 위한 시설확보에 필요한 기술과 장비개발의 진행을 위해 국제항해선박 및 항만시설의 보안에 관한 법률 시행규칙을 시행하고 있지만 안정화되기까지는 시간이 소요된다고 볼 수 있다

항만물류분야에서 보안과 관련된 기존의 연구로는 해운항만법제적 측면의 관점에서 항만보안법제 개선과 관련된 연구가 있으며(Bang, 2013), 해상보안관리적 측면에서의 정보관리 위험분석모델을 개발하기 위한 연구가 있었다(Jeong, 2012). 또한 Park(2016)는 항만그룹 대상으로 평가한 보안과 관련한 재정투자가 효과성과 효율성을 중심으로 하는 항만성과에는 긍정적인 영향을 나타내었지만 항만이용자그룹을 대상으로 분석한 결과 부정적 영향을 주는 것으로 나타났기에 항만그룹과 항만이용자들간의 인식의 문제점에 차이가 있다는 부분에 대해서 인식 관련 보안교육의 중요성을 언급하였다.

2.2 조직보안 관련 연구

조직보안과 관련된 연구로는 다음과 같다. Choi(2015)의 연구에서 조직문화의 관계적 문화, 혁신적 문화가 조직몰입 직무만족에 유의하게 영향을 미치고 있다는 것을 확인할 수 있었다. 또한 관계적 문화는 보안정책준수의지에도 관련성이 있었다. Choi(2015)은 조직의 정보보호 수준에 영향을 미치는 요소는 조직의 담당자의 역할에 따라 다를 수 있음을 확인하고자 하였다. 분석결과 보안업무비중이 높은 조직의 담당자가 보안업무 비중이 낮은 조직의 담당자보다 정보보호 수준의 정도가 높다는 것으로 분석되었다.

Kim(2015)은 정보보안 관리에 대한 신뢰에 기여하는 주요요인으로 경영자 지원이 정보보안정책과 정보보안 자원 가용성에 영향을 미치는 주요 선행요인으로 검증되었으며, 정보보안정책은 관리적 차원에서의 정보보안의 신뢰에 중요한 영향을 미치는 요인으로 분석되었다. Layton(2005)은 정보보안인식은 정보보안행동에 영향을 미친다고 하였으며, 정보보안태도는 개인적 특성에 따라 보안인식의 정보가 다르게 나타남을 확인하였다. Knapp et al.(2005)은 정보보안효과성은 최고 관리자의 지지도 필요하지만 조직의 정보보호를 위한 정책이라는 요소가 무엇보다 중요함을 나타내었다.

3. 연구설계

3.1 연구모형

본 연구에서는 항만물류조직구성원들의 정보보안능력에 영향을 미치는 요인을 분석하고자 Bulgurcu et al.(2010)의 정보보안 정책 준수이론을 기반으로 연구모형을 설정하였다. Bulgurcu et al.(2010)의 연구에서는 계획된 행동이론을 바탕으로 조직의 정보보안정책을 준수를 장려하기 위한 조직의 노

력을 정보보안정책과 준수 관련 신념의 역할에 대한 방향으로 연구를 하였다. 항만물류분야의 조직구성원들의 보안능력에 영향을 미치는 요인을 분석한 연구는 미흡하였으며 조직차원의 접근방법이 아닌 연속적인 정보의 흐름을 지원하는 조직구성원들의 체계적인 보안관리가 필요하다고 판단하였다. 이에 본 연구에서는 정보보안인식에 영향을 미치는 선행 요인으로 보안규범과 보안활동의 요인으로 선정하였으며, 정보보안능력에 영향을 미치는 선행요인으로는 보안규범과 보안인식으로 구성하였다. 따라서 다음의 연구모형<그림 1>과 같이 구성하였다.

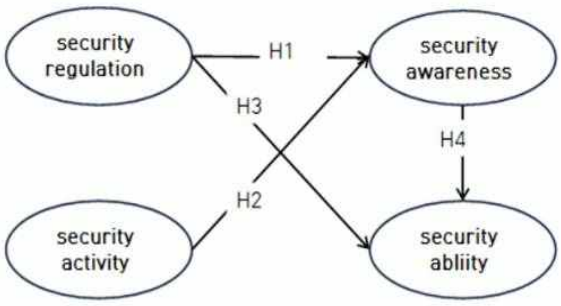


Fig. 1 Research model

3.2 연구가설

보안규범은 보안의 위협으로 인해 사용자, 네트워크 및 데이터를 보호하기 위한 전략을 구축하기 위한 전반적인 접근방식을 활용하는 규범이다. 조직의 보안규범은 안전한 조직의 정보를 보호하기 위한 환경을 유지하는 수준 높은 인식을 가지는데 영향력이 있다. Berejikian(2002)는 조직의 역할을 잘 수행해 나가기 위한 방법으로 조직의 규범을 잘 이행하지 않았을 경우 받게되는 처벌도 규범사항에 속하는 범위라고 하였다. Lebow and Stein(1990)는 처벌에 대한 확실성과 엄격성에 따라서 바람직한 행위가 이행될 수 있음을 강조하며 처벌에 대한 규범의 조정이 필요함을 제시하였기에 조직구성원의 보안인식에 영향을 미치는 선행요인으로 보안규범을 처벌 관련 항목으로 선정하였다. 따라서 다음과 같은 연구가설1을 도출하였다.

[가설1] 보안규범은 조직구성원들의 보안인식에 정(+)의 영향을 미친다.

정보보안활동은 기업의 중요한 정보자산을 보호하기 위해 외부로부터 발생할 위협으로부터 예방적인 차원에서 관리할 수 있는 활동의 영역이다. 조직의 자산에 해를 끼치는 손실과 피해를 최소화하기 위한 보안정책을 이해하고 이를 실천하기 위한 활동이 무엇보다 필요하다(Bulgurcu et al., 2010). 조직 내에서 정보보안 활동을 위해 필요한 정책사항들에 대한 이해는 선행되어야 할 사항이다. 그 이후 정보보안정책에 대한 원칙에 따른 정보보안 활동들이 조직구성원 모두에게 공포되어야 한다. 보안활동은 조직의 임무와 규모, 역할, 운영방식에 따라 조직의 목표와 특성에 부합한 정책(Halibozek and Kovacich, 2005; Siponen, 2000)으로 구성되어야 한다. 보안활동이 잘 이루어진다면 조직구성원들의 보안인식에 긍정적인 영향을 미칠 것이다. 보안활동에 포함되어있는 조직과 관련된 사항들이 보안인식을 제고시키는데 중요하게 작용한다. 따라서 다음과 같은 가설2를 도출하였다.

[가설2] 보안활동은 조직구성원들의 보안인식에 정(+)의 영향을 미친다.

Drevin et al.(2007)연구에서 정보보안을 행할 때 정보노출에 대한 대응조치는 개인의 보안능력으로 평가할 수 있다고 하였다. 이는 정보자산의 중요성을 인식하는 수준에 대한 보안능력을 측정할 수 있으며 정보보안 위협의 가능성을 인식하는 수준도 개인의 보안능력 정도에 따라 다르다는 것을 확인하였다. Lim(2006)는 정보보안의 중요성을 인식하는 것은 조직의 정보보안을 위한 시스템 프로세스에 대한 관리적 부분을 포괄하는 부분이라고 강조하였다. 관리적인 부분이라는 것은 보안능력의 정도로 평가할 수 있다. Nosworthy(2000)는 효과적인 정보보안을 위해 사전에 시행되어야 하는 정보보안 관련 교육과 훈련의 중요성도 언급하였으며, 정보보안인식의 제고를 위한 노력향상에 기여하는 보안관리 즉, 개인의 보안능력을 향상시키는 것이 중요하다는 것을 언급하였다. 또한 Knapp et al.(2005)은 정보보안정책과 관련된 정보효과는 개인적인 상황요인들로부터 발생할 수 있는 부분임을 강조하였기에 개인의 보안능력을 향상시키기 위한 방안도 중요하다. Choi et al.(2008)은 보안정책과 절차, 보안 훈련 및 교육, 접근제어, 시스템과 프로그램 업데이트, 보안팀 구성이 조직구성원들의 보안능력에 긍정적인 효과가 있다고 하였다. 조직은 조직정보의 유입과 유출에 대한 내역 관리, 방화벽, 인증 등의 보안규범의 인적관리가 중요하다. 조직의 보안규범을 준수하지 않으면 이에 대한 처벌의 사항들에 대한 권고적인 조치의 보안규범은 조직구성원들의 보안능력을 향상시키는데 긍정적인 영향을 미칠 것이다. 따라서 다음과 같은 가설3을 도출하였다.

[가설3] 보안규범은 조직구성원들의 보안능력에 정(+)의 영향을 미친다.

조직구성원들의 조직보안에 대한 신뢰는 개인이 조직을 위해 준수해야 하는 보안정책 관련 사항들에 대한 인식의 정도 차이에서부터 발생한다. 정보보안능력은 정보보안관리에 대한 인식적인 부분(Nance and Straul, 2008)과 기술적으로 활용할 수 있는 방안(Stanton et al., 2005), 보안사고 발생 시 해결할 수 있는 능력(Woo, 2012)이다. 정보보안인식의 중요성이 높다

는 것은 정보의 침해로부터 보호하기 위해 사용되는 대책 및 솔루션에 대한 보안능력에 높다는 것이다. 조직구성원들의 보안인식의 수준이 높으면 이에 대한 보안사항에 대한 이해도가 높다는 것으로 판단할 수 있으며 보안관련 대처할 수 있는 보안능력 향상에 긍정적인 영향을 미칠 수 있다 따라 따라서 다음과 같은 가설4를 도출하였다.

[가설4] 보안인식은 조직구성원들의 보안능력에 정(+)의 영향을 미친다.

3.3 연구변수의 조작적정의 및 측정항목

연구모형의 가설설정에 사용하기 위한 각 구성개념들에 대한 조작적 정의한 측정항목은 다음과 같다. 보안규범은 조직의 보안정책과 같은 정보보안규범을 준수하지 않았을 경우 처벌을 받게 되는 정도라고 조작적 정의를 내렸으며, 측정항목으로는 상위관리자통보에 대한 처벌, 시스템사용제한의 처벌, 불이익에 대한 처벌, 업무활동제한의 처벌로 구성하였다. 보안활동은 조직의 보안활동으로부터 나타나는 긍정적인 특성이라고 조작적 정의를 내렸으며, 측정항목으로는 보안활동의 적용성, 보안활동의 행동성, 보안활동의 유용성, 보안활동의 효과성으로 선정하였다.

보안인식은 보안기술이나 보안관리를 위해 필요한 사항들에 대해 조직구성원들이 인식하는 정도라고 조작적 정의를 내렸으며, 측정항목으로는 정보자산의 중요성인식, 정보보안위협의 인식, 정보보안취약성의 인식, 정보보안 관리의 인식으로 선정하였다. 보안능력은 보안을 위한 사전 문제점을 검토하고 보안문제점 발생 시 해결하고 기술을 적용할 수 있는 능력의 정도라고 조작적 정의를 내렸으며, 측정항목으로는 정보보안 피해 대처능력, 보안시스템 해결능력, 보안해결을 위한 신속한 능력, 보안해결을 위한 판단능력으로 선정하였다. 모든 설문항목은 리커트(Likert) 7점 척도로 구성하였다.

4. 실증분석

4.1 표본설계와 자료수집

항만물류조직의 정보보안능력에 영향을 미치는 요인을 실증적으로 분석하여 검정하기 위해 표본 집단으로 항만물류조직에 종사하고 있는 조직구성원들을 대상으로 설문을 수행하였다. 총 130개의 설문지를 배부하여 130개의 설문지를 회수하였으며, 결측치가 있거나 불성실하게 응답한 설문지 11부를 제외한 총 119부가 본 연구의 최종분석에 사용되었다. 응답자의 인구통계적 특성을 분석한 결과는 Table 1과 같다.

Table 1 Demographic characteristics

Division	Item	Frequency (Person)	Ration (%)
Gender	Man	96	80.7
	Woman	23	19.3
Age	20～30 under	16	13.4
	30～40 under	56	47.1
	40～50 under	37	31.1
	50 above	10	8.4
Organization type	Shipping company & Forwarding	73	61.3
	Terminal company & Operating company	46	38.7
Position	Staff	17	14.3
	Administrative Manager	40	33.6
	Section Manager	39	32.8
	Manager	21	17.6
	Director	2	1.7

4.2 측정모형의 신뢰성 및 집중타당성

본 연구에서는 기존의 타당성이 인정된 연구모형을 재검증하는 확인적 성향의 연구로 측정모형의 추정과 분석을 위하여 확인적 요인분석으로 측정모형을 추정하고, 구조모형을 2단계 접근법을 실시하였다. 이를 위해 구조방정식 모형의 1단계 분석에서 확인적 요인분석을 통해 측정모형을 추정하였으며 분석을 위한 구조방정식 모형을 검증하기 위해 AMOS 20.0을 사용하였다. 항만물류조직구성원을 대상으로 분석한 구성개념별 단일차원성을 저해하는 측정변수는 표준화 잔차와 수정지수로 출력된다. 표준화 잔차가 유의한 수준을 지나치게 벗어나거나 수정지수의 값이 5를 넘어서는 측정변수들 간의 관계에 대해서 각 측정항목들을 모형의 타당성 검정을 위해서 단계적으로 제거해 나가는 방법을 사용하여 확인적 요인분석을 실시하였다. 확인적 요인분석을 통해 추출된 16개의 측정항목 중에서 보안인식3, 보안능력4의 항목이 표준화된 잔차와 수정지수가 크게 나타나 이들 항목을 제외한 14개의 항목을 최종적으로 구조방정식을 이용한 측정 하부모형을 실증분석하였다.

본 연구의 측정 하부모형의 신뢰성을 평가하기 위해 합성개념신뢰도, 평균분산추출 값, Cronbach-α 값을 Table 2에 제시하였다.

Table 2 Measurement model analysis

Variable	Convrgent Validity						
	Estimate	t value	Standar-dized Estimate	Measure-ment Error	Internal Coposite Reliabil-ity	AVE	Cronbach-α
SR1	0.82	9.40	0.81	0.34	0.92	0.72	0.85
SR2	0.87	9.94	0.81	0.35			
SR3	0.82	10.26	0.82	0.33			
SS4	1		0.95	0.10			
AW1	0.93	6.88	0.84	0.30	0.84	0.63	0.79
AW2	1		0.72	0.48			
AW4	0.95	6.97	0.82	0.33			
AC1	0.93	12.69	0.85	0.28	0.91	0.73	0.85
AC2	1		0.94	0.12			
AC3	0.86	12.16	0.89	0.20			
AC4	0.83	8.76	0.72	0.49			
AB1	0.59	5.06	0.56	0.69	0.81	0.59	0.76
AB2	1		0.87	0.24			
AB3	0.91	6.59	0.84	0.30			

각 구성개념들에 대하여 지정된 예측변수가 그들 구성개념을 충분히 설명하고 있는가를 확인하는데 필요한 추정치는 합성개념 신뢰도와 평균분산추출 값(Average Variance Extracted: AVE)이다. 본 연구에서 각 구성개념들에 대하여 지정된 예측변수가 그들 구성개념을 충분히 설명하고 있는가를 확인하는데 필요한 추정치인 합성개념 신뢰도가 구성개념의 권장수준 0.7이상으로 모두 상회하는 결과를 나타났다. 평균분산추출값(AVE)은 권장수준 0.5이상을 상회하였기에 모두 양호한 결과로 확인하였다. 내적신뢰도에서 Cronbach-α 값이 권장기준 0.7이상의 수용기준에 부합되었으며 내적신뢰성이 확보되었음을 알 수 있다. 집중타당성 결과를 살펴보면 측정항목의 추정치가 0.5이상이며, 그 추정치의 t-값이 2.0이상일 때, 측정항목의 집중타당성이 있는 것으로 판단한다. 모든 항목들의 추정치와 그 추정치의 t-값은 권고되는 수치를 충분히 만족시키는 것으로 나타나 연구에 적용된 항목들의 집중타당성은 충분히 있다고 판단할 수 있다.

4.3 측정모형의 판별타당성

다음은 측정모형의 판별타당성 결과이다. 각 구성개념들의 평균분산추출 값의 제곱근이 다른 구성개념들 간의 상관계수보다 상회하는 것으로 나타나 판별타당성을 검증하였으며 아래의 Table 3에 제시하였다.

Table 3 Determination Validity(AVE)

Construct	AVE			
	1	2	3	4
1.SS	(0.85)			
2.AC	0.55	(0.85)		
3.AW	0.26	0.56	(0.79)	
4.AB	0.27	0.34	0.35	(0.77)

4.4 측정모형과 구조모형의 적합도

측정모형의 적합도와 구조모형에 대한 적합도 지수를 나타낸 결과는 아래의Table 4에 나타내었다.

Table 4 Goodness of fit index

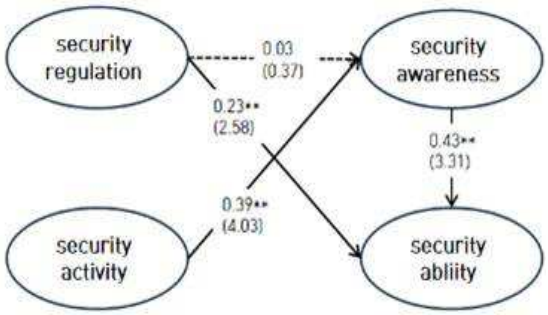
Division	Fit Index	Acceptance Standard	Measurement Model	Structure Model
Absolute Fit Index	χ^2/df	≤3.00	1.03	1.71
	χ^2		71.34	122.86
	df		69	72
	p-value	≥0.05	0.00	0.00
	GFI	≥0.90	0.95	0.88
	RMSEA	≤0.08	0.02	0.08
Incremental Fit Index	AGFI	≥0.80	0.87	0.82
	TLI	1.0근사	0.98	0.93
	IFI	1.0근사	0.99	0.95
	CFI	≥0.90	0.99	0.95
Parsimony Fit Index	PGFI	≥0.60	0.60	0.60
	PNFI	≥0.60	0.54	0.70

측정모형에 있어서 χ^2(p)는 71.34(0.00)이고, χ^2을 자유도로 나눈 비율이 1.03로 나타나 권장수준(≤3.00)을 만족시키는 것으로 분석되었다. GFI가 0.91, AGFI가 0.87로 권장수준에 적합하게 나타났으며 RMSEA 값이 0.02로 권장수준을 만족하였다. 그리고 1.0에 근사할 경우 적합하다고 볼 수 있는 IFI가 0.99, TLI가 0.98, CFI가 0.99, 간명부합지수 PGFI, PNFI가 각각 0.60, 0.54로 나타났다. PNFI가 권장수준보다 조금 낮게 나타났지만 이를 제외한 적합도 지수가 대체적으로 측정모형의 적합도가 수용기준을 충족하는 것으로 평가하였다. 구조모형에 대한 적합도 지수를 보면 χ^2(p)는 122.85(0.00)이고, χ^2을 자유도로 나눈 비율이 1.71으로 나타나 권장수준(≤3.00)을 만족시키는 것으로 분석되었다. 측정모형 결과와 유사하게 GFI가 0.88, AGFI가 0.83으로 권장수준에 만족하였다. RMSEA 값이 0.08로 권장수준을 만족하고, 1.0에 근사할 경우 적합하다고 볼 수 있는 IFI가 0.95, TLI가 0.93, CFI가 0.95, 간명부합지수 PGFI, PNFI가 각각 0.60, 0.70으로 나타나 권장수준에 부합하는 결과로 분석되었다.

4.5 구조모형의 검증결과

구조모형의 분석결과에 따른 연구가설 검정결과를 각 경로의 추정치와 t-값으로 다음의 Fig. 2와 같이 나타났다. 보안처

벌규정에서 보안인식에 이르는 연구가설1(H1) 경로를 제외한 다른 모든 경로는 통계적으로 유의한 것으로 확인되어 연구가설 검정결과가 채택되었다. 우선, 보안규범이 보안인식에 영향을 미치는 요인을 설정한 연구가설1(H1)을 제외한 다른 모든 경로는 통계적으로 유의한 것으로 확인되었으며, 연구가설 검증결과에 대한 요약은 아래의 Table 5와 같다.



주)( ): t-value, **: p<0.01

Fig. 2 Results of research model

Table 5 Results of hypothesis testing

Hypothesis	Path coefficient	t-Value	Results
[H1]	0.03	0.37	Rejection
[H2]	0.39	4.03**	Adoption
[H3]	0.23	2.58**	Adoption
[H4]	0.43	3.31**	Adoption

5. 결 론

물류체계의 내·외부적인 관점에서 의도적인 보안사고를 사전에 방지하거나 위해 사태 발생에 대해 복구 조치를 수행하는 것은 국가물류체계에서 중요한 활동이다. 항만과 물류조직의 보안의 중요성은 글로벌 공급사슬 전체에도 강조되어야 하는 사항이다. 특히 항만물류관리에 대한 광범위한 ICT기반의 운영 및 통제도 중요하지만 세부적인 인적보안의 틀에서 통제되어야 하는 조직의 보안사항들에 대한 검토도 필요한 시점이다. 이에 본 연구는 항만물류조직 구성원들의 보안능력에 영향을 미치는 요인을 도출하여 확인할 수 있었다. 조직구성원들의 보안활동은 조직구성원들이 보안인식에 긍정적인 영향을 가져다주었고 보안규범과 보안인식도 보안능력향상에 긍정적인 영향을 미치는 결과로 나타났다. 반면 보안규범은 보안인식에 유의하지 않은 결과로 나타났다. 이는 보안규범에 대한 측정항목이 처벌과 관련된 보안규범 항목이었기에 부정적인 측면의 규범이 보안인식에 영향을 미치는 것은 아니라는 것을 확인할 수 있었다. 조직구성원들의 사기가 향상될 수 있는 긍정적인 요인들에 규범이 보안인식에 대한 수준향상에 필요할 것으로 보인다. 즉, 조직에서는 처벌의 관점이 아닌 보상이라는 차원에서 긍정적인 인센티브 요소들을 제공할 수 있는 보안규범의 항목들을 제시할 필요성이 있다. 이는 조직의 정보보안을 위한 조직구성원들의 보안관련 규정의 참여도를 높이는데 기여할 것이며 이로 인한 조직의 중요자산에 대한 보안관리적 차원의 조직구성원들의 사기 향상과 업무의 생산성 향상에도 기여할 것이다.

본 연구의 한계점과 향후 연구방향은 다음과 같다. 첫째, 조직구성원들의 보안능력에 영향을 미치는 요인을 조직의 제도적인 관점에 국한하여 결과를 분석하였다는 것이다. 향후 연구에서는 보다 다양한 관점에서의 요인들을 도출하여 비교·분석할 필요성이 있다. 둘째, 해운항만물류 분야의 조직의 특성상 나타난 결과이다. 추후 연구에서는 일반기업에도 적용하여 기업특성별 구분하여 결과에 대한 비교·분석 및 해석하는 연구가 진행되어야 할 것이다. 끝으로 항만물류조직별 설문이 아닌, 개인 대상 설문에 내재된 한계점을 있다. 보안인식과 보안능력은 개인 단위 측정이 의미가 있지만, 동일한 조직에서 보안규범의 엄격성이나 보안활동 수준의 평가는 주관적일 수 있기에 추후 연구에서는 조직적측면과 개인적측면의 관점에서 비교·분석하는 연구가 시행되어야 할 것이다.

References

[1] Anderson, C. L. and Agarwal, R.(2010), "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions", MIS Quarterly, Vol. 34, No. 3, pp. 613-643.

[2] Bang, H. S. and Ju, J. K.(2013), "A Study on an Improvement in Korean Port Security Related Laws", Maritime Law Review, Vol. 25, No. 1, pp. 153-178.

[3] Berejikian, J. D.(2002), "A Cognitive Theory of Deterrence", Journal of Peace Research, Vol. 39, No. 2, pp. 165-183.

[4] 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.

[5] Choi, N., Kim, D., Goo, J. and Whitmore, A.(2008), "Knowing is Doing: An Empirical Validation of the Relationship between Managerial Information Security Awareness and Action", Information Management and Computer Security, Vol. 16, No. 5, pp. 484-501.

[6] Choi, D. K., Song, M. S., Im, J. I. and Lee, K. H.(2015), "Study the role of information security personnel have on an organization's information security level", Korea Institute Of Information Security And Cryptology, Vol. 25, No. 1, pp. 197-209.

[7] Choi, Y. H.(2015), "The Effect of Organizational Culture

on Organizational Commitment, Job Satisfaction, and Willingness to Comply with the Industrial Security Policies", The Korean Association of Police Science Review, Vol. 17, No. 6, pp. 343-366.

[8] Drevin, L., Kruger, H. A. and Steyn, T.(2007), "Value Focused Assessment of ICT Security Awareness in an Academic Environment", Computers and Security, Vol. 26, No. 1, pp. 36-43.

[9] Jeong, W. L.(2012), "A Study on the Development of Analysis Model for Maritime Security Management", Journal of Navigation and Port Research, Vol. 36, No. 1, pp. 9-14.

[10] Kang, J. Y.(2013), "A Study on the Systematized and Unified Plan of Port Logistics Security Management System", Journal of Law and Politics research, Vol. 13, No. 2, pp. 389-436.

[11] Kim, S. H. and Song, Y. M.(2011), "An Empirical Study on Motivational Factors Influencing Information Security Policy Com- pliance and Security Behavior of End-Users (Employees) in Organizations", The e-Business Studies, Vol. 12, No. 3, pp. 327-249.

[12] Kim, S. Y., Choi, J. H. and Kim, C. H.(2009), A Study on Measures to Develop the Port Logistics Security Industry, Korea Maritime Institute.

[13] Kim, Y. J.(2015), "Key Determinants of Employees' Trust toward Information Security Management in an Organization",The Journal of Internet Electronic Commerce Resarch, Vol. 15, No. 4, pp. 247-264.

[14] Knapp, K. J., Marshall, T. E., Rainer, R. K. and Ford, F. N.(2005), Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness, White Paper, Information Systems Security Certification Consortium (ISC), 2.

[15] Ko, H. J.(2011), "A Study on the Implications and Trends of Logistics Security Assurance Programs for International Trade Facilitation", Korean Institute of Navigation and Port Research, Vol. 27, No. 2, pp. 333-354.

[16] Layton, T.(2005) ,Information Security Awareness: The Psychology Behind the Technology, Author House.

[17] Lee, H. G.(2009), "A Study on the Evaluation of the Information Security Level in Major Container Terminals", Journal of Navigation and Port Research, Vol. 33, No. 1, pp. 45-50.

[18] Lim. C. H.(2006), "Effective Information Protection Recognition Improvement Plan", Korea Institute Of Information Security And Cryptology , Vol. 16, No. 2, pp. 30-36.

[19] Ministry of Maritime Affairs and Fisheries (2013), Rules for the enforcement of the Act on the Security of International Navigation Ships and Port Facilities.

[20] Ministry of Maritime Affairs and Fisheries (2016), Prepare the basis for strengthening port security, such as the system for allowing ships to enter and leave.

[21] Park, M. K.(2007), "Study on Remodeling Korean Logistics Laws for Strengthening Integration and Adjustment Function of Logistics Policy", Journal of Korea Port Economic Association, Vol. 23, No. 2, pp. 63-86.

[22] Park, H. K.(2016), "Impact of Security Related Financial Investment on Port Performance through Relationship Management: Focused on Ports and Port Users", Korea Logistics Review , Vol. 26, No. 5, pp. 67-78.

[23] Rogers, R. W.(1983) Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In: Cacioppo, J. and Petty, R., Eds., Social Psychophysiology, Guilford Press, New York, pp. 153-177.

[24] Shim, W. H.(2011), "Analysis of the Impact of Security Liability and Compliance on a Firm's Information Security Activities", The Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 53-73.

[25] Siponen, M. T.(2000), "A Conceptual Foundation for Organization Information Security Awareness", Information Management and Computer Security, Vol. 8, No. 1, pp. 31-41.

[26] Siponen, M., Pahnila, S. and Mahmood, M. A.(2010), "Compliance with Information Security Policies: An Empirical Investigation", Computer, Vol. 43, No. 2, pp. 64-71.

[27] Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J.(2005), "Analysis of End User Security Behaviors", Computers and Security, Vol. 24, No. 2, pp. 124-133.

[28] Woo, S. H.(2012), "A Study on Security Capability of IDPS", The Institute of Electronics and Information Engineers-CI, Vol. 49, No. 4, pp. 9-15.

[29] Workman, M. and Gathegi, J.(2007), "Punishment and Ethics Deterrents: A Study of Insider Security Contravention", Journal of the American Society for Information Science and Technology, Vol. 58, No. 2, pp. 212-222.

Received 19 March 2019
Revised 2 April 2019
Accepted 8 April 2019