한국항해항만학회지 제40권 제4호
J. Navig. Port Res. Vol. 40, No. 4 : 213-222, August 2016 (ISSN:1598-5725(Print)/ISSN:2093-8470(Online))
DOI : http://dx.doi.org/10.5394/KINPR.2016.40.4.213

해운항만조직의 정보보안이행이 정보보안성과에 미치는 영향

강다연* · † 장명희

* 동명대학교 해운경영학과 겸임교수, † 한국해양대학교 해운경영학부 교수

The Influence of Information Security Behaviors on Information Security Performance in Shipping and Port Organization

Da-Yeon Kang · † Myung-Hee Chang*

** Division of Shipping Management, Tongmyong University, Busan 608-711, Korea*
† Division of Shipping Management, Korea Maritime and Ocean University, Busan 49112, Korea

요 약 : 최근 조직의 정보유출사고가 연이어 발생하면서 조직차원에서 정보보안 관리와 정보보안대책 수립이 시급하다. 특히 조직구성원들의 정보보안 관리 강화 방안을 마련하고 조직구성원들의 정보보안 인식의 제고를 위해 노력을 기울여야 한다. 조직의 정보보안이행 정도가 정보보안성과에 미치는 영향을 확인하기 위한 연구모형을 설정하였으며, 표본 집단으로 해운·항만조직과 금융·보험 조직의 구성원들을 선정하였다. 구조방정식 모형을 이용하여 결과요인을 도출하였으며 설문지를 통해 수집된 데이터를 실증적으로 분석하였다. 해운·항만조직 구성원을 대상으로 정보보안성과에 영향을 미치는 요인을 분석한 결과는 다음과 같다. 첫째, 정보보안인식에 영향을 미치는 요인으로 정보보안태도, 정보보안관심도로 확인되었으며, 둘째, 조직의 정보보안정책에 영향을 미치는 요인으로는 정보보안규범인 것으로 확인되었다. 반면에 정보보안처벌과 정보보안교육은 정보보안정책 준수에 영향을 미치지 않는 것으로 확인되었다. 셋째, 정보보안인식은 정보보안정책준수, 정보보안능력, 정보보안행동에 유의한 영향을 미치는 것으로 확인되었다. 넷째, 정보보안정책준수는 정보보안능력과 정보보안행동에 영향을 미치는 요인으로 확인되었다. 마지막으로 정보보안능력과 정보보안행동은 정보보안성과에 영향을 미치는 요인으로 확인되었다.

핵심용어 : 정보보안인식, 정보보안행동, 정보보안정책, 정보보안성과

Abstract : *Recently, as cases of organizations' information disclosure occur continuously, it is urgent to manage security of information and establish measures to enhance security of information by an organization itself. Especially, members of an organization should be prepared with measures for information security, and an organization should do its efforts to raise its members' awareness toward information security. I set a research model to verify what effects an organization's fulfillment of regulations to secure information brings to performance of information security and selected members from maritime and port organizations and financial and insurance institutes as sample. Results of the analysis to identify factors affecting information security performance among members of maritime and port organizations are as follows. Firstly, I found that the factors affecting information security awareness are information security attitude and information security standards. Secondly, the factor giving influence on information security policy of an organization was found to be information security standards. In contrast, information security punishments and information security training were verified not to give influence on compliance of information security policy. Thirdly, information security awareness was identified to give significant influence on compliance of information security policy, information security competence and information security behavior. Fourthly, compliance of information security policy was verified to be those factors that give influence on information security competence and information security behavior. Lastly, information security competence and information security behavior were found to be such factors that give influence on information security performance.*

Key words : *Information security awareness, Information security behavior, Information security policy, Information security performance*

1. 서 론

정보보안의 체계는 물리적 보안, 기술적 보안, 관리적 보안으로 나누어진다. 기업들은 보안을 위해 종종 기술기반의 솔루션들에 투자하고 이에 의존하여 왔으나 정보보안과 관련된 위험들을 충분히 제거하지 못했다. 물리적, 기술적 보안도 중요하지만 관리적 보안이 무엇보다 더 중요하게 평가되어야 하는 부분이다. 조직의 자산에 해를 끼칠 수 있는 위험요소인 보

* 연회원 : mswcrash@hanmail.net 051)629-1412
† Corresponding author : 종신회원, cmhee2004@kmou.ac.kr 051)410-4384

안위협은 조직의 내부적·외부적 요인들에 대한 노출, 변조, 파괴, 불법사용으로 인해 발생한다. 명확한 조직의 정보보안관리를 위한 조직구성원들의 정보보안지식 관련 보안능력 향상과 보안행동을 가져다주기 위해 우선적으로 보안인식에 대한 제고가 요구된다(Chen et al., 2008).

우선 정보보안을 위한 조직구성원이 반드시 준수해야 할 관리적 보안은 조직의 정보자산 사용에 대한 무지와 실수를 하지 않아야 하며, 조직정보자산에 대한 관리를 부당한 목적으로 악용하는 행동을 행하지 않아야 한다. 또한 조직구성원들이 조직 정보보안 위협에 대한 부분을 소홀히 관리하는 것도 조직보안에 심각한 피해를 가져다준다는 것을 간과해서는 안 된다. 따라서 조직의 정보보안을 위해서는 무엇보다 조직구성원의 정보보안 실천이 가장 중요한 요구사항이라고 볼 수 있다(Siponen, 2000).

조직의 정보보안을 측정하기 위한 선행요인으로 개인적인 차원의 특성과 조직적인 차원의 특성 모두를 고려해 정보보안이행에 따른 조직의 정보보안성과를 측정한 논문은 없었다. 조직의 정보보안을 행하는 조직구성원들의 정보보안인식을 측정함과 동시에 조직의 정보보안정책을 준수하는 조직적 특성요인을 기반으로 조직의 정보보안이행을 정확하게 측정할 필요성이 있다(Siponen et al., 2010). 조직에 속한 개인의 정보보안인식 정도와 정보보안정책준수 여부는 조직의 정보보안 성과에 영향을 미치게 된다. 특히 조직의 정보보안정책준수 여부는 조직의 정보보안성과를 위한 지침이지만 조직에 속한 개인이 이행하는 정도에 따라 조직의 정보보안성과가 달라질 것이다.

본 연구는 정보보안 이행의 관점을 개인과 조직차원에서 측정할 수 있는 요인을 분류하여 조직의 정보보안성과에 영향을 미치는 요인을 실증 분석하는 연구로 기존 연구와의 차별성을 두었다. 따라서 본 연구의 목적은 개인의 보안인식에 영향을 미치는 요인과 조직의 보안정책준수정도에 영향을 미치는 요인을 바탕으로 조직보안 능력 향상과 정보보안을 이행할 수 있는 보안행동을 측정하였다. 또한 이러한 분석을 통해 조직의 정보보안성과에 영향을 미치는 요인을 최종적으로 도출하고자 한다.

2. 이론적 배경

2.1 해운·항만조직의 보안 현황 및 대책

해운·항만조직 내의 정보의 특징은 다음과 같다. 우선 영업정보의 보안으로 운임, 송장, 가액, 화물정보 등을 다루고 있는 부분에서 업무적인 정보보안이 요구된다. 전략정보의 보안으로는 조직의 영업 전략, 화물 별 전략 등의 정보가 유출되지 않게 관리하여야 한다. 개인 및 기업의 정보보안을 위해서는 조직의 내부 데이터베이스의 유출에 대한 피해를 발생시키지 않도록 정보보안이 요구된다고 볼 수 있다.

해운·항만에서의 인터넷비즈니스의 사용이 확대되면서 정보 의존율이 심화되고 있는 상황이며 이는 정보 단절과 누락, 정보 유출 시 해운·항만 업무의 차질이 전체적인 정보시스템을 다루며 진행하는 인터넷비즈니스 근간에 위협이 발생할 수 있다는 것이다. 이러한 위협을 사전에 조치를 취하기 위한 방법으로 현재의 정보통신 인프라스트럭처 하에서는 보안이 조직의 생존을 유지시키기 위한 필수 조건이라는 것을 말해준다. 해운·항만분야내의 정보는 화물, 기업, 개인, 정부의 정보가 유기적으로 얽혀있다. 정보 보안의 취약성이 존재하고 있으며, 일반 기업에 비하여 체계적인 보안전략이 없다는 것이다. 또한 해운·항만 관련 IT기업의 다양성 부족으로 인한 기업의 정보보안대책이 이루어지고 있지 않은 실정이다.

해운·항만분야의 보안을 위한 내부적인 전략으로 관리적 보안, 물리적 보안, 시스템 보안의 관점으로 대응책을 마련해야 한다. 우선 관리적 보안부분에서는 정보보호를 위한 조직구성원의 보안관리 수준과 관련 조직체계 및 관련 계획을 수립해야 한다. 조직의 보안을 지원하는 조직을 구성하며 정보보호 정책을 수립하고 인적보안에 대한 통제가 이루어져야 한다. 물리적 보안으로는 정보보호를 위한 물리적 통제수준과 물리적 피해에 대비한 설비를 수축하여야 한다. 이는 보안제한 구역을 관리하거나 접근 통제 기술을 적용하여 대비할 수 있다. 시스템 보안으로는 정보시스템 보안을 위한 기술적인 대책을 수립하는 것이다. 백업 및 복구 시스템을 완비하고 네트워크 및 O/S보안, DB 및 응용 SW적용과 시스템 접근 통제가 실시되어야 한다(Kang, 2013). 해운·항만산업에서의 정보기술은 다른 산업 보다 신속하게 도입하고 있으며, 정보기술의 도입으로 산업의 효율화를 달성하고 있다. 특히, 화주, 선사 및 포워더, 운송사, 컨테이너터미널 운영사, 관세청, 국토해양부 등 다양한 주체가 공급망을 구축하고 있고 정보의 흐름이 단절될 경우 공급망 전체에서 업무 마비가 일어날 수 있는 상황이다. 정보보안의 관리가 무엇보다 중요하며 시급하게 해결해야 과제이기 때문에 조직의 정보보안 관리적 측면에서의 인적보안요소를 통제할 수 있는 정보보안성과를 위한 해결방안이 마련되어야 한다.

최근 연이어 발생하여 큰 사회적 문제로 대두되고 있는 개인정보유출사고가 항만물류 행정에서도 발생한 개연성을 차단에 차단할 목적으로 인천항만청은 인천청과, 인천항만공사 및 인천항보안공사 등의 시스템에 대한 개인 정보보호 실태를 일제 점검하고, 항만청 내 보안시스템을 최신 시스템으로 교체하고 직원들에게 개인정보보호교육을 실시하고 있다. 개인정보가 유출되지 않도록 지속적으로 점검하고 교육을 실시해 나갈 계획에 맞춰 조직구성원들에게 정보보안 강화 대책을 마련의 중요성이 시급하다.

2.2 정보보안인식과 정보보안이행 관련 연구

정보보안인식은 정보보안 이슈에 대한 개인의 관심의 정도로 정보보안에 대한 자각 및 정보보안활동에 대한 관심 정도

라고 할 수 있다(Choi et al., 2008). Siponen(2000)은 정보보안 인식의 증가는 사용자와 관련된 실수를 최소화 할 것이고 사용자 관점의 보안 기술 및 절차의 효율성을 최대화 할 것이라고 주장하였다. 조직 구성원의 정보보안 중요성에 대한 인식이 전제되지 않은 상태에서 정보보안 기술 자체가 조직의 정보자원을 효과적으로 보호해 줄 수는 없다. Chen et al. (2008)은 보안인식은 인간요소에 포함되어 있으며 이제는 기술적 보안 솔루션뿐만 아니라 인간이 정보자산 보호의 중요 요소라고 주장했다. 실제로 보안위협은 사용자의 지식과 행동의 부주의와 결핍에 그 직접적인 원인이 있으므로 오늘날의 정보보안의 성공에 있어 보안 인지는 기술적 요소보다 더 중요할 수도 있다는 것이다.

정보보안인식제고는 조직의 정보자산에 대한 조직 구성원의 정보보안을 보안정책에 따라 적절한 정보보안인식제고를 수행하여야 한다. 결국 정보보안인식제고는 자산, 정책, 정보보안인식교육이 실행되어야 하는 것이다. 이상 살펴본 많은 연구에서 정보보안인식은 보안위협으로부터 정보 시스템을 보호하는데 가장 중요한 요소이고 조직의 전체적인 정보보안 성과에 매우 큰 영향을 미치는 요인이라고 주장하고 있다.

정보보안인식에 대한 선행연구들을 살펴보면 다음과 같다. Goodhue & Straub (1991)는 보안 관심 모형을 제시하며 사용자의 정보보안에 대한 관심에 영향을 미치는 요인들에 대한 연구하였다. 이 연구에서 정보시스템에 대한 적정한 수준의 관심과 인지도는 합리적인 보안 대책 선정의 전제조건이라고 가정하고 정보보안에 대한 관심에 영향을 미치는 요인들에 대하여 연구하였다. 이들은 실증연구를 통해 정보시스템의 오용에 대한 조직 관리자의 인식과 정보 시스템의 사용에 대한 인식 제고와 교육이 사용자의 정보보안 서비스에 만족에 영향을 미친다는 결과를 발표하였다.

Nosworthy(2000)는 정보보안의 실패가 정보보안에 대한 인식 미비, 자원 할당부족 및 교육 및 훈련 부족에 기인한다고 하였다. 따라서 정보보안의 실패를 방지하기 위해서는 정보보안의 인식 제고 및 교육, 훈련이 필요하다는 것이다. Knapp et al.(2005)은 정보보안 효과인지에 대한 개인중심의 영향요인을 분석하여 최고관리자의 지지, 사용자의 훈련, 보호문화, 정책관련성, 정책적 강제 등이 인지된 정보보안의 효과성에 미치는 영향을 증명하였다.

Bulgurcu et al.(2010)은 정보보안정책준수에 있어 정보보안인식과 지각된 공정성의 역할'이라는 실증연구를 통해서 정보보안인식과 지각된 공정성이 태도에 영향을 주는 것을 밝혀내고 조직의 정보보안 규칙과 규정을 따르게 하는데 조직구성원들의 정보보안인식과 공정성의 역할을 증명하였다.

2.3 정보보안성과 관련 연구

정보보안성과에 대한 연구를 살펴보면 정보보안 사고 발생빈도 및 피해예방에 대한 연구가 주를 이루고 있다. 정보보안성과란 조직이 정보보안관리 통제 또는 활동을 통해 얻고자 하는 목적으로 정보보안 사고의 예방 및 손실 방지와 같은 소극적 목적으로부터 경쟁우위, 공공이미지, 고객 만족과 같이 정보보안과 관련된 적극적 목적이 있을 수 있다. Straub & Collins(1990)의 연구에서는 관리자가 사용자에게 정보시스템의 사용과 관련하여 허용되는 행위와 허용되지 않는 부적절한 행위에 대해 사용자들에게 공지하고, 허용되지 않는 정보시스템 오·남용에 대해서는 벌칙을 부여할 경우 사고발생의 횟수, 기회비용 손실 등이 축소되는 것으로 확인하였다. 또한 예방적 보안대책과 같은 정보보안에 대한 투자는 컴퓨터 오남용에 따른 막대한 손실을 현저하게 감소시킬 수 있음을 지적하였다.

Sun(2005)은 정보화 성과 연구와 같이 포괄적인 시각에서 조직 내외 이해당사자들의 정보보안 만족도와 같은 역량 강화를 포함하여 정보보안성과를 도출하였다. 연구결과 정보보안성과를 정보보안 사고 빈도를 줄임으로써 얻는 사고빈도 감소성과, 자산의 손실을 줄이는 자산관리 성과, 비즈니스 기회 손실 감소로 얻는 비즈니스 기회성과, 타사 경쟁 시 손실 감소로 얻는 타사경쟁 성과, 이미지 실추 손실 감소로 얻는 이미지성과를 도출하였다. Kim & Ahn(2013)은 정보보호문화, 규범적 신념, 행위, 가치가 정보보호 규정 위반 행위에 어떠한 영향을 미치는지 실증분석 하였다. 아노미 개념을 토대로 조직 내에서 정보보호 규정의 중요성에 대한 인식 결핍과 정보보호 규정의 가치 결여를 정보보호 아노미현상으로 정의하고 이 현상이 어떠한 역할을 하는지 수행하였다. 연구결과 자신이 속한 기업이 정보보호 규정에 대한 관심이 높다고 생각할수록 정보보호 아노미에 대한 인신 수준은 낮아졌으며 정보보호 규정에 대해 조직원이 유용하다고 느끼는 정도가 높을수록 정보보호 아노미에 대한 인식 수준은 낮아지는 것으로 나타났다.

3. 연구 설계

3.1 연구모형

본 연구에서는 조직의 정보보안성과에 영향을 미치는 요인들을 분석하기 위하여 개인의 정보보안인식측면과 조직의 정보보안정책준수 관점으로 분류하였으며, 이에 따른 조직의 정보보안 이행과의 관련성에 살펴보고 정보보안성과에 영향을 미치는 요인으로 구성하여 연구모형을 제시하였다. 조직구성원들의 정보보안인식과 조직의 정보보안정책준수에 따른 조직의 정보보안 이행을 정보보안능력 및 정보보안행동으로 구성하여 정보보안성과와의 관계를 살펴보고자 하였으며, 분석하고자 하는 연구모형은 다음의 Fig. 1과 같다.

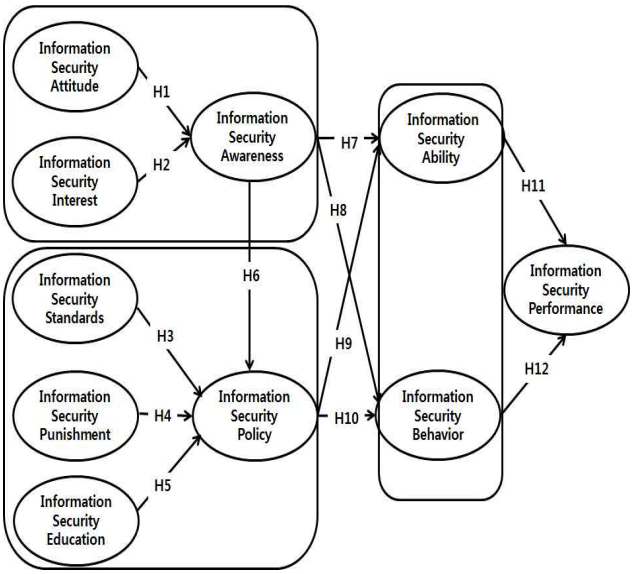


Fig. 1 Research model

3.2 연구가설

3.2.1 정보보안인식과 선행요인간의 관계

정보보안인식에 영향을 미치는 요인으로 정보보안태도와 정보보안관심도를 선행요인으로 도출하였다. 조직의 정보보안을 위한 정보보안태도는 조직구성원이 수행할 수 있는 조직정보보안 관련 활동 등에 대한 호의적인 태도로 보았으며(Layton, 2005; Workman & Gathegi, 2006), 정보보안태도가 형성되어 있을 때 조직의 정보보안위험성에 대해 대처할 수 있는 정보보안인식의 정도가 높아짐을 설명하고자 한다(Hong et al., 2003). 조직구성원들의 정보보안관심도는 조직의 정보보안활동을 위해 보안관련 사항들에 대한 관심정도를 의미하며(Carrie et al., 2004), 조직의 정보보안관심도가 높다면 조직의 정보보안위험성에 대한 보안 관리대처에 관한 정보보안인식에 긍정적인 영향을 미치게 될 것이다(Chen et al. 2008). 정보보안관심도는 정보보안 관련 최신정보에 관심이 있는지 여부와 조직 정보시스템을 안전하게 관리하기 위해 습득해야 하는 보안방법에 대한 관심이 높아져 보안활동에 적극적으로 참여하기도 한다. 조직구성원들의 정보보안관심도가 높으면 정보보안인식을 가질 수 있을 것이다. 따라서 다음과 같은 가설1과 가설2를 도출하였다.

[가설1] 조직구성원들의 정보보안태도는 정보보안인식에 정(+)의 영향을 미친다.

[가설2] 조직구성원들의 정보보안관심도는 정보보안인식에 정(+)의 영향을 미친다.

3.2.2 정보보안정책준수와 선행요인간의 관계

정보보안규범은 조직 문화를 잘 파악해 조직특성을 이해하고 보안사항을 반영하여 규범이 잘 규정되었는지에 따라 조직의 보안정책을 준수 이행에 도움이 될 것이다(Kang & Chang, 2012). 정보보안처벌이 조직에 규정되어 있다면 조직구성원들은 부정적인 영향을 받는 것에 대한 거부감이 발생하기에 이를 회피하기 위해 조직의 정보보안정책을 잘 이행하는데 긍정적인 영향을 미칠 것이다(Lebow & Stein, 1990; Berejikian, 2002). 조직의 정보보안교육은 조직구성원들에게 정보보안과 관련된 보안특강이나 정보보안에 관한 훈련을 실시하는 것이며(Choi et al, 2008), 조직은 정보보안교육에 대한 세미나를 조직구성원들에게 정기적으로 실시하는 것이 중요하다(Park, 2012). 정보보안교육을 잘 수행했다면 조직의 정보보안정책준수사항을 반드시 받아들여하며 이행해야 한다는 것을 알게 될 것이다(Nosworthy, 2000). 따라서 정보보안정책준수에 영향을 미치는 선행요인으로 정보보안규범, 정보보안처벌, 정보보안교육과 관련된 가설3, 가설4, 가설5를 다음과 같이 수립하였다.

[가설3] 조직의 정보보안규범은 보안정책준수에 정(+)의 영향을 미친다.

[가설4] 조직의 보안처벌은 보안정책준수에 정(+)의 영향을 미친다.

[가설5] 조직의 보안교육은 보안정책준수에 정(+)의 영향을 미친다.

3.2.3 정보보안인식과 정보보안정책준수 간의 관계

조직구성원들의 정보보안인식의 정도가 높으면 조직의 정보보안정책을 준수하는 정도가 높아질 것이다(Yim, 2012). 조직의 정보보안에 대한 사항들을 잘 알고 있기 때문에 기업이 보유하고 있는 자산정보를 다양한 위협으로부터 보호하고 중요한 정보유출이 발생하는 것을 예방하고자 할 것이다(Park & Kim, 2011; Drevin et al., 2007). 이는 조직의 가치와 조직자산에 대한 손실과 피해를 최소화하기 위한 조직의 지침과 가이드라인으로 규정되어 있는 정보보안정책준수로 확인할 수 있다(Bulgurcu et al., 2010). 따라서 조직구성원의 정보보안인식은 정보보안정책준수에 긍정적인 영향을 미친다고 가설6을 도출하였다.

[가설6] 조직구성원들의 정보보안인식은 보안정책 준수에 정(+)의 영향을 미친다.

3.2.4 정보보안능력과 선행요인 간의 관계

조직구성원들의 정보보안인식은 조직의 정보자산에 가해질

정보보안 위협을 인식하는 것은 조직 정보보안에 대한 취약성과 정보보안 시스템 관리를 할 수 있는 정보보안능력의 정도가 높아진다는 것이다(Woo, 2012; Nance & Straul, 2008). 정보보안인식은 조직구성원들의 정보보안 사항과 관련된 피해의 정도를 확인한 후, 조직의 정보보안해결방법에 대한 능력을 향상시키는데 긍정적인 영향을 미친다고 할 수 있다(Stanton et al., 2005; Choi et al., 2008).

정보보안정책준수사항을 잘 이행한다면 최소한 관리되어야 할 정보보안사항에 대한 요소를 확인할 수 있다. 이를 통해 정보보안정책을 위반하지 않고 잘 이행한다면 조직의 정보보안 목표와 부합되는 정보보안능력 수준이 향상될 것이다(Park & Yim, 2012).정보보안정책만 잘 이행하는 것은 정보보안능력 향상에 긍정적인 영향을 미친다는 것을 확인하고자 한다. 따라서 조직구성원들의 정보보안능력에 영향을 미치는 선행요인으로 정보보안인식과 정보보안정책준수로 선정하여 가설7과 가설8을 도출하였다.

[가설7] 조직구성원의 정보보안인식은 정보보안능력에 정(+)의 영향을 미친다.

[가설8] 조직의 보안정책준수는 정보보안능력에 정(+)의 영향을 미친다.

3.2.5 정보보안행동과 선행요인 간의 관계

정보보안행동은 조직의 정보보안을 실행하기 위한 조직구성원들의 실천적인 행동사항이다(Kim & Song, 2011).조직구성원들이 조직의 정보보안에 대한 지각된 인식수준이 높으면 정보보안을 위해 실천해야 하는 사항들을 반영하여 정보보안을 위한 노력을 이행하는 행동사항의 정도가 높아질 것이다(Lee et al. 2004; Chen et al., 2008).

조직의 정보보안정책 사항을 준수하는 것은 조직의 정보보안과 관련된 정책기반 업무사항의 적용성 향상에도 기여한다(Geordie & David, 2012). 또한 조직의 보안활동 행동의 유용성과 효과성에 대한 도움을 주고자하는 사항을 포함하고 있기에 조직의 정보보안을 위한 행동에 긍정적인 영향을 미칠 것이다. 따라서 정보보안행동에 영향을 미치는 선행요인으로 정보보안인식과 정보보안정책준수로 선정하여 다음과 같은 가설9, 가설10을 수립하였다.

[가설9] 조직구성원의 정보보안인식은 정보보안행동에 정(+)의 영향을 미친다.

[가설10] 조직의 보안정책준수는 정보보안행동에 정(+)의 영향을 미친다.

3.2.6 정보보안성과와 선행요인 간의 관계

조직의 정보보안성과는 조직 내/외부적인 피해의 손실을 감소시키고 효과적인 조직 보안을 평가할 수 있는 성과적인 측면을 확인하는 사항으로 확인할 수 있다(Ha & Kim, 2013). 조직 보안사고 발생에 대한 피해의 손실을 감소시킬 수 있는지 정보유출 피해 규모에 대한 감소, 조직의 정보보안 안전성과 조직의 보안관리 요구사항에 대한 충족도로 평가한다(Park, 2007). 조직구성원들의 보안능력수준이 높다는 것은 조직의 정보보안성과를 높이는데 영향을 미칠 것이다.

조직구성원들의 조직 정보보안을 위한 행동은 조직보안 사항을 사전에 실천하고 이행하는 것이다. 조직의 정보보안성과로 확인할 수 있는 조직의 정보보안사고 손실에 대한 감소와 정보유출피해 규모의 감소, 조직정보보안의 안전성과 조직 내 정보보안 요구사항 충족도의 향상으로 확인할 수 있으며(Kankanhalli et al., 2003; Geordie & David, 2012), 이는 정보보안성과에 긍정적인 성과를 가져다 줄 것이다. 따라서 조직의 정보보안성과와의 관계에서 영향력 있는 선행요인으로는 정보보안능력, 정보보안행동으로 선정하여 다음과 같은 가설11과 가설12를 수립하였다.

[가설11] 조직구성원들의 정보보안능력은 정보보안성과에 정(+)의 영향을 미친다.

[가설12] 조직구성원들의 정보보안행동은 정보보안성과에 정(+)의 영향을 미친다.

3.3 연구변수의 조작적 정의 및 측정변수

본 연구모형과 가설설정에 사용한 구성개념에 대한 조작적 정의와 측정항목은 다음과 같다. 우선 정보보안태도는 호의적인 정보보안태도를 형성하기 위해 조직구성원이 수행할 수 있는 조직정보보안을 위한 행동으로 조작적 정의를 내렸으며, 측정항목으로는 스팸메일필터링, 컴퓨터의 안전성 확인, 패스워드 비노출, 백신설치로 구성하였다. 정보보안관심도는 조직의 정보보안 활동을 위한 보안 관련 사항들의 관심정도라고 조작적 정의를 내렸으며, 측정항목으로는 정보보안 최신정보 습득의 관심도, 정보보안 프로그램 업데이트에 관한 관심도, 해커 침투 가능성의 관심도, 개인정보 도용 피해우려의 관심도로 선정하였다.

정보보안규범은 조직 내 규정된 정보보안규범이 정보보안을 위해 잘 규정되었다고 생각하는 긍정적인 측면의 정도라고 조작적 정의를 내렸다. 측정항목으로는 정보보안의 안전성, 신뢰성, 우수성, 업무보안 적용성으로 선정하였다. 정보보안처벌은 정보보안규범을 준수하지 않았을 때 돌아오는 불이익이 가해 질 수 있는 정도라고 조작적 정의를 내렸으며, 상위관리자의 통보처벌, 시스템 사용 제한의 처벌, 불이익에 대한 처벌, 업무활동의 제한의 처벌로 구성하였다. 정보보안교육은 조직의 정보보안교육에 대한 조직구성원들의 인지된 효용성 정도라고 조작적 정의를 내렸으며, 정보보안교육의 유익성, 적합성, 정보보호 활동성, 조직 업무적용성으로 측정항목을 선정하

였다.

정보보안인식은 조직에서 발생할 수 있는 정보보안 위험성에 대한 보안기술이나 보안관리 대처에 대한 조직구성원들의 인식정도라고 조작적 정의를 내렸다. 정보보안인식을 측정하기 위한 항목으로는. 조직 정보자산의 중요성, 조직 정보보안 위협인식, 조직 보보안취약성 인식, 조직 정보보안 시스템 관리 중요성 인식 등으로 선정하였다. 정보보안정책준수는 조직의 정보보안과 관련된 정책, 가이드라인을 준수할 때 정보보안 활동에 도움을 주는 사항의 정도라고 조작적 정의를 내렸다. 측정항목으로는 보안정책기반 업무보안의 적용성, 보안정책기반 보안활동 행동의 유용성, 보안정책기반 보안활동 확인의 유용성, 보안정책기반 보안황동확인의 효과성으로 구성하였다. 정보보안능력은 조직의 정보보안 사항에 대해 이해하며, 해결할 수 있고 정보보안기술을 적용할 수 있는 능력의 정도라고 조작적 정의를 내렸다. 측정항목으로는 정보보안 피해인식, 정보보안 기술사용방법, 정보보안기술 활용도, 정보보안 문제해결로 구성하였다. 정보보안행동은 조직의 정보보안을 실행하기 위한 조직구성월등의 실천적인 행동사항 정도라고 조작적 정의를 내렸으며, 측정항목으로는 정기적인 패스워드 변경, 정보보호실정, 업무문서차기, 출처가 명확한 파일 다운로드로 선정하였다.

마지막으로 정보보안성과는 조직의 정보보안 활동으로 인한 조직 내부적, 외부적인 피해의 손실을 감소시키고 조직보안을 평가할 수 있는 성과 사항이라고 조작적 정의를 내렸다. 이를 측정하기 위한 항목으로는 조직의 정보보안사고 손실 감소, 조직의 정보유출 피해 규모 감소, 조직정보보안의 안전성 확보, 조직정보보안 관련 요구사항 충족도 향상으로 구성하였다. 모든 측정항목은 리커트(Likert) 7점 척도로 설문항목을 구성하였다.

4. 실증분석

4.1 표본설계와 자료수집

조직의 정보보안성과에 영향을 미치는 요인을 실증적으로 분석하기 위한 표본 집단으로 해운항만조직에 종사하고 있는 조직구성원들을 대상으로 설문을 수행하였다. 본 연구는 구조방정식 모형을 이용하여 인과요인을 도출하였으며 수집된 데이터를 실증 분석하였다. 총 150개의 설문지를 배부하여 150개의 설문을 회수하였으며, 결측치가 있거나 불성실하게 응답한 설문지 5부를 제외한 총 145부가 본 연구의 최종분석에 사용되었다.

Table 1은 해운・항만조직 응답자의 조직보안 관련 특성이다. 조직 내 보안전담조직이 유/무에서 있다가 113명(77.9%), 없다가 32명(22.1%)로 나타났다. 보안정책 유/무에서는 있다가 135명(93.1%), 없다가 10명(6.9%)로 분석되었다. 또한 보안처벌은 있다가 110명(75.9%), 없다가 35명(24.1%)로 분석되었다. 연간 보안교육을 받는 횟수는 1회가 59명(40.7)로 가장 높은 비율을 차지하고 있었으며 2~3회가 54명(37.2%)으로 나타났다.

Table 1 Characteristics of the sample

Division		Frequency (Person)	Ration (%)
Security Organization	existence	113	77.9
	nonexistence	32	22.1
Security Policy	existence	135	93.1
	nonexistence	10	6.9
Security Punishment	existence	110	75.9
	nonexistence	35	24.1
Security Education (Annual)	1	59	40.7
	2~3	54	37.2
	4~5	19	13.1
	6 or more	13	9
Total		145	100

4.2 측정모형의 신뢰성과 집중타당성 평가

해운・항만조직의 표본 집단을 대상으로 분석한 구성개념별 단일차원성을 저해하는 측정변수는 표준화 잔차와 수정지수로 나타난다. 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 40개의 측정항목 중에서 정보보안태도에서 SA2 항목, 정보보안관심도에서 SI1, 정보보안규범에서 SS3, 정보보안처벌에서 SP3, 정보보안교육에서 SE2, 정보보안인식 AW3, 정보보안정책준수에서 POL3, 정보보안능력 AB1, 정보보안행동 SB2, 정보보안성과 항목에서 ISP4 항목의 10개의 항목이 표준화된 잔차와 수정지수가 크게 나타나 이들 항목을 제외한 30개의 항목에 대하여 최종적으로 구조방정식을 이용한 측정 하부모형을 실증 분석하였다.

본 연구의 측정 하부모형의 신뢰성을 평가하기 위해 합성개념신뢰도, 평균분산추출 값, Cronbach-α 값을 Table 2에 제시하였다. 구성개념에 의해 설명되는 분산의 양을 나타내는 평균분산추출 값(AVE)이 0.5를 상회하며, 각 측정항목의 추정치가 0.5이상, 그 추정치의 t-값이 2.0이상으로 나타나 집중타당성이 높은 것을 확인하였으며, Cronbach-α 값이 0.7이상으로 나타나 수용기준에 부합하는 결과를 확인하였다.

Table 2 Measurement model analysis

Construct	Convergent Validity							
	Variable	Estimate	Standardized Estimate	t value	Measurement Error	Internal Composite Reliability	AVE	Cronbach-α
1. SA	SA1	0.97	0.76	8.76	0.44	0.78	0.55	0.74
	SA2	1	0.84	-	0.28			
	SA4	0.68	0.61	7.23	0.62			
2. SI	SI1	0.65	0.57	2.90	0.67	0.77	0.54	0.72
	SI3	0.65	0.69	5.63	0.54			
	SI4	1	0.92	-	0.19			
3. SS	SS2	0.99	0.93	19.16	0.15	0.93	0.83	0.91
	SS3	1	0.93	-	0.13			
	SS4	0.92	0.87	16.43	0.24			
4. SP	SP1	0.86	0.78	11.06	0.40	0.87	0.69	0.83
	SP2	1	0.89	-	0.21			
	SP4	0.93	0.83	12.07	0.32			
5. SE	SE1	0.85	0.89	15.97	0.21	0.9	0.76	0.87
	SE2	1	0.92	-	0.16			
	SE4	0.86	0.80	12.93	0.35			
6. AW	AW1	0.96	0.83	11.03	0.32	0.83	0.62	0.78
	AW2	0.92	0.66	8.69	0.58			
	AW4	1	0.86	-	0.26			
7. POL	POL1	0.63	0.89	5.21	0.21	0.88	0.71	0.84
	POL2	0.64	0.92	5.26	0.15			
	POL4	0.57	0.72	4.89	0.50			
8. AB	AB1	0.66	0.65	8.58	0.58	0.84	0.64	0.79
	AB2	0.90	0.83	12.02	0.30			
	AB3	1	0.90	-	0.20			
9. SB	SB2	0.68	0.67	5.75	0.55	0.77	0.53	0.75
	SB3	1	0.82	-	0.48			
	SB4	0.97	0.74	6.37	0.43			
10. ISP	ISP1	0.91	0.89	17.76	0.22	0.9	0.75	0.86
	ISP2	1	0.96	-	0.06			
	ISP3	0.80	0.75	12.47	0.46			

4.3. 측정모형의 판별 타당성 평가

아래의 Table 3에 제시된 측정모형의 판별타당성 결과를 보면 각 구성개념들의 평균분산추출 값의 제곱근이 다른 구성개념들 간의 상관계수보다 상회하는 것으로 나타나 판별타당성을 확인하였다. 한 구성개념 내에서의 측정항목들은 자체 로딩한 값이 다른 구성개념과의 크로스 로딩한 값보다 큰가를 측정하여 판별타당성을 검증 하였다.

Table 3 Determination Validity(AVE)

Construct	AVE									
	1	2	3	4	5	6	7	8	9	10
1. SA	(0.74)									
2. SI	0.45	(0.73)								
3. SS	0.18	0.32	(0.91)							
4. SP	0.24	0.44	0.57	(0.83)						
5. SE	0.2	0.52	0.65	0.65	(0.87)					
6. AW	0.61	0.31	0.48	0.34	0.47	(0.78)				
7. POL	0.31	0.30	0.71	0.56	0.62	0.59	(0.85)			
8. AB	0.44	0.52	0.51	0.40	0.65	0.56	0.48	(0.8)		
9. SB	0.40	0.36	0.52	0.44	0. 53	0.64	0.69	0.6	(0.73)	
10. ISP	0.32	0.24	0.57	0.65	0.64	0.54	0.53	0.61	0.59	(0.87)

4.4. 모형의 적합도 평가

Table 4는 측정모형의 적합도와 구조모형에 대한 적합도 지수를 나타낸 결과이다. 우선 측정모형에 있어서 χ^2(p)는 551.28(0.00)이고, χ^2을 자유도로 나눈 비율이 1.55로 나타나 권장수준(≤3.00)을 만족시키는 것으로 분석되었다. GFI가 0.814, AGFI가 0.76으로 권장수준보다 조금 낮게 나타났지만 연구모형이 얼마나 잘 근사하느냐의 정도를 나타내는 RMSEA 값이 0.06으로 권장수준을 만족하였다. 그리고 1.0에 근사할 경우 적합하다고 볼 수 있는 IFI가 0.93, CFI가 0.93, 간명부합지수 PGFI, PNFI가 각각 0.62, 0.68로 나타났으며 적합도 지수 모두 대체적으로 측정모형의 적합도가 수용기준을 충족하는 것으로 평가하였다.

다음으로 구성개념의 구조적 관계를 설명하는 구조모형에 대한 적합도 지수를 보면χ^2 (p)는 584.62(0.00)이고, χ^2을 자유도로 나눈 비율이 1.57로 나타나 권잠수준(≤3.00)을 만족시키는 것으로 분석되었다. 측정모형 결과와 유사하게 GFI가 0.808, AGFI가 0.76으로 권장수준보다 조금 낮게 나타났지만 연구모형이 얼마나 잘 근사하느냐의 정도를 나타내는 RMSEA 값이 0.06으로 권장수준을 만족하고, 1.0에 근사할 경우 적합하다고 볼 수 있는 IFI가 0.93, CFI가 0.93, 간명부합지수 PGFI, PNFI가 각각 0.65, 0.7로 나타나 권장수준에 부합하는 것으로 분석되었다.

Table 4 Goodness of fit index

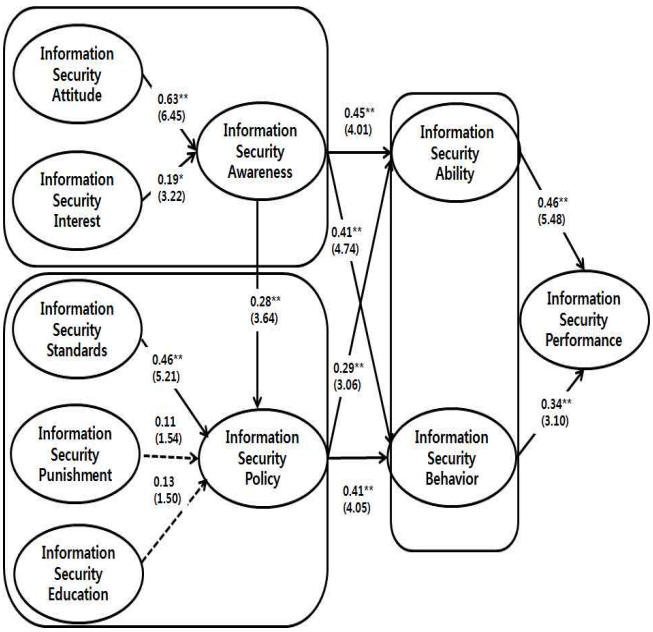
Division	Fit Index	Acceptance Standard	Measurement Model	Structure Model
Absolute Fit Index	χ^2/df	≤3.00	1.55	1.57
	χ^2		551.28	584.62
	df		356	373
	p-value	≥0.05	0.00	0.00
	GFI	≥0.90	0.814	0.808
	RMSEA	≤0.08	0.06	0.06
Incremental Fit Index	AGFI	≥0.80	0.76	0.76
	NFI	≥0.90	0.83	0.82
	RFI	1.0근사	0.79	0.79
	IFI	1.0근사	0.93	0.93
	CFI	≥0.90	0.93	0.93
Parsimony Fit Index	PGFI	≥0.60	0.62	0.65
	PNFI	≥0.60	0.68	0.7

Table 5 Results of hypothesis testing

Hypothesis	Path coefficient	t-Value	Results
H1	0.63	6.45**	Adoption
H2	0.19	3.22*	Adoption
H3	0.46	5.21**	Adoption
H4	0.11	1.54	Rejection
H5	0.13	1.50	Rejection
H6	0.28	3.64**	Adoption
H7	0.45	4.01**	Adoption
H8	0.41	4.74**	Adoption
H9	0.29	3.06**	Adoption
H10	0.41	4.05**	Adoption
H11	0.46	5.48**	Adoption
H12	0.34	3.10**	Adoption

4.5. 구조모형 검증 결과

구조모형의 분석결과에 따른 연구가설 검정결과를 각 경로의 추정치와 t-값으로 나타내면 다음의 Fig. 2에서 보는 바와 같다. 정보보안처벌과 정보보안정책준수 간의 관계를 검정하는 연구가설4(H4) 경로와 정보보안교육이 정보보안정책준수에 영향을 미친다는 연구가설5(H5)를 제외한 다른 모든 경로는 통계적으로 유의한 것으로 확인되어 연구 가설들이 채택되었다. 최종적인 가설 검증 결과는 Table 5와 같다.



주) ( ): t-Value, *: p<0.05, **: p<0.01

Fig. 2 Results of research model

5. 결 론

본 연구를 통해 해운·항만조직 구성원들이 정보보안에 대한 긍정적인 보안태도를 가지고 정보보안관심도를 높게 보일 때 조직의 정보보안인식 수준에 영향을 미친다는 것을 확인할 수 있다. 조직의 정보보안규범은 해운·항만 조직의 특성상 정보보안을 위한 관리적인 측면에서 접근할 수 있는 허용범위를 조직의 유형별로 조직의 특성별로 각각의 보안규범이 명시되어 있다. 해운·항만의 시설보안에 대한 규범이 아닌 정보보안에 관한 규범이기에 정보자산에 대한 중요성을 인식했을 때 정보보안정책을 반드시 준수하게 되는 것이다.

해운·항만조직의 정보보안처벌과 정보보안교육은 실제로 형식적으로 규정되어 있고 시행하는 경우가 대부분이며 교육비율이 높지 않다는 것을 알 수 있다. 조직에서의 근로계약을 맺을 때나 매년 연봉계약을 체결할 때 보안과 관련해 지켜야 하는 사안을 설명해주는 것도 중요하다고 할 수 있다. 단순히 정보보안교육과 처벌에 대한 사항을 직원들을 모아놓고 하는 것보다, 실무적인 차원에서 맨투맨으로 교육하는 방법도 필요하다고 본다. 정보보안을 위한 인식의 정도가 높을 때 정보보안정책을 준수하는데 영향력이 있다는 것을 확인하였다. 정보보안을 인식한다는 것 자체가 정보보안능력과 행동을 위한 단계적인 정보보안활동에 영향을 주는 부분이라고 볼 수 있다.

정보보안정책을 준수한다는 것은 조직에서 강조되고 반드시 지켜야하는 준수사항에 대해 이해하고 검토한 부분이 충분히 높다고 판단할 수 있으며 이는 조직구성원들의 효과적인 정보보안을 위한 관리적인 측면의 정보보안능력과 행동으로 표출된다는 것을 알 수 있다. 정보보안능력의 수준이 높고 정보보안행동이 이뤄진다는 것은 조직의 정보보안에 대한 손실

을 감소시킬 수 있는 방안으로 모색하고 정보보안을 위한 조직의 성과지향을 위해 공동의 목표를 달성할 수 있다고 볼 수 있다.

본 연구의 의의로는 다음과 같다. 해운·항만조직 보안의 특성으로 연간 보안교육을 시행하는 횟수가 1회가 40.7%, 2~3회가 37.2%로 나타나 해운항만 정보보안 유출시 파급효과에 대한 피해는 심각성에 대한 조직의 보안교육에 대한 관리가 시급함을 알 수 있었으며, 보안교육의 강화와 함께 조직구성원에게 조직보안의 중요성과 위험에 대한 심각성을 인식시킬 필요성을 알려주었다. 또한 금융·보험조직의 특성상 정보보안을 위한 교육체계가 잘 이뤄지고 있음에도 불구하고 정보보안 유출 관련 사고가 빈번히 발생하는 현 시점에서 가장 체계적인 정보보안을 행하고 있는 조직의 구성원들의 정보보안성과에 영향을 미치는 요인을 확인하면서 정보보안인식의 제고를 가져다주기 위한 연구를 수행하였다는 점이다.

본 연구의 한계점과 향후 연구방향은 다음과 같다. 첫째, 조직의 정보보안성과에 영향을 미치는 요인을 분석하기 위한 요소를 정성적인 측면으로만 접근하여 분석하였다는 것이다. 향후 실질적인 기업의 정량적인 접근의 방식으로 정보보안성과에 영향을 미친 요인을 비교하며 기업의 재무데이터 기반으로 정보보안성과에 대한 비교와 분석이 필요할 것이다.

둘째, 개인의 정보보안인식이 조직의 정보보안정책준수에 영향을 미치는 요인을 검정하기 위한 가설을 수립한 경로에서 개인의 인지적 차원이 조직의 정보보안성과에 영향을 가져다주는 것으로 판단하였다. 추후 연구에서는 조직의 정보보안정책준수가 조직구성원들의 개인적 차원인 정보보안인식에도 영향력을 가져다주는지 확인하기 위한 연구가설을 수립하여 검증할 필요성이 있다.

References

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

[2] Bulgurcu, B., Cavusoglu, H., and Benbasat I.(2010), “Information Security Policy Com- pliance: An Empirical Study of Rationality -Based Beliefs and Information Security Awareness”, MIS Quarterly, Vol. 34, No. 3, pp. 523-548.

[3] Chen, C. C., Medlin, B. D., and Shaw, R. S.(2008), “A Cross-Cultural Investigation of Situational Information Security Awareness Programs”, Information Management and Computer Security, Vol. 16, No. 4, pp. 360-376.

[4] 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.

[5] 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.

[6] Frank, J., Shamir, B. and Briggs, W.(1991), “Security-related Behavior of PC Users in Organizations”, Information and Management, Vol. 21, No. 3, pp. 127-135.

[7] Goodhue, D. L. and Straub, D. W.(1991), “Security Concerns of System User: A Study of Perceptions of the Adequacy of Security”, Information and Management, Vol. 20, No. 1, pp. 13-27.

[8] Govindarajan, V. and Fisher, J(1990)., “Strategy, Control Systems, and Resource Sharing: Effects on Business-unit Performance”, The Academy of Management Journal, Vol. 33, No. 2, pp. 259-285.

[9] Ha, S. W. and Kim, H. J.(2013), “The Effects of User’s Security Awareness on Password Security Behavior”, Journal of Digital Contents Society Vol. 14 No. 2, pp. 179-189.

[10] Kang, D. Y. and Chang, M. H.(2012), “Factors Influencing on the Compliance of Information Security Policy of Workers of Shipping and Port Organization”, The Korea Port Economic Association, Vol. 28, No. 1, pp. 1-23.

[11] 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.

[12] Kankanhalli, A., Teo, H. H., Tan, B. C. Y. and Wei, K.(2003), "An Integrative Study of Information Systems Security Effectiveness”, International Journal of Information Manage- ment, Vol. 23, No. 2, pp. 139-154.

[13] Kim, H. j. and Ahn, J. H.(2013), “An Empirical Study of Employee’s Deviant Behavior for Improving Efficiency of Information Security Governance”, Society for e-Business Studies, Vol. 18, No. 1, pp. 147-164.

[14] 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.

[15] 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), Vol. 2.

[16] Layton, T.(2005), Information Security Awareness : The Psychology behind the Technology, AuthorHouse.

[17] Lebow, R. and Stein. J.(1990), "Deterrence: The Elusive Dependent Variable", World Politics, Vol. 42, No. 3, pp. 336-369.

[18] Lee, S. M., Lee,. S. G. and Yoo. S.(2004), "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories", Information and Management, Vol. 41, No. 6, pp. 707-718.

[19] Lee, S. J. and Lee, M. J.(2008), "An Exploratory Study on the Information Security Culture Indicator", Informatization policy, Vol. 15, No.3, pp.100-119.

[20] Nosworthy, J.(2000), "Implementing Information Security in the 21st Century-do You Have the Balancing Factors?", Computer and Security, Vol. 19, No. 4, pp. 337-347.

[21] Park, C. J. and Yim, M. S.(2012), "An Understanding of Impact of Security Counter- measures on Persistent Policy Compliance", The Society of Digital Policy & Management, Vol. 10, No. 4, pp. 23-35.

[22] Park, I. B. and Kim, J. D.(2011), "A Study on the Policy Management for Industrial Security's Culture", The Journal of Korean Association for Industry Security, Vol. 2, No.1, pp. 33-46.

[23] Park, J. Y.(2012), "An Analysis on Training Curriculum for Educating Information Security Experts", Management Information Systems Review, Vol. 31, No. 1, pp.149-165.

[24] Park, S. S.(2007), "Concept of Strategy in Organizational Information Security", Journal of Information and Security, Vol. 7, No. 3, pp. 15-24.

[25] Rezgui, Y., and Marks, A.(2008), "Information Security Awareness in Higher Education: An Exploratory Study", Computers and Security, Vol. 27 No. 7-8, pp. 241-253.

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

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

[28] 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.

[29] Sun, H. G.(2005), "Impacts of Information Security Policies and Organizations on the Information Security Performance in Korean Enterprises", The Korea Society of Management Information Systems proceedings, Vol. 2005, No. 1, pp. 1087-1095.

[30] 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.

[31] Workman, M., and Gathegi, J.(2006), "Puni- shment 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.

[32] Yim, M. S.(2012), "A Path Way to Increase the Intention to Comply with Information Security Policy of Employees", The Society of Digital Policy & Management, Vol. 10, No. 10, pp. 119-128.

Received 20 June 2016
Revised 9 August 2016
Accepted 29 August 2016