Journal of Korea Port Economic Association, Vol.30, No.1, 2014, 97-118.

정보보안정책 준수가 정보보안능력 및 행동에 미치는 영향 분석 : 해운항만조직 구성원을 대상으로

강다연* · 장명희**

An Analysis of Compliance with Information Security Policy Effects on Information Security Ability and Behavior : Focused on Workers of Shipping and Port Organization

Dayeon Kang · Myunghee Chang

Abstract : Recent accidents of customer information leakage increase the necessity of information security for organization and the importance of information security team for it. To strengthen information security, organizations make information security policy and ask the members to comply with it. In this regard, maritime organization also needs to structure information security policy and examine its ability and behavior. The purpose of this study is to analyze the effects of compliance with information security policy on the ability and behavior of workers in shipping and port organization. The results of investigation show that information security education and norm affect compliance with information security of the workers. On the contrary, the punishment of information security is insignificant. It is shown that the degree of compliance with information security significantly affects its ability and behavior of the workers in shipping and port organization.

Key Words : Shipping and Port Organization, Information Leakage, Compliance with Information Security Policy, Information Security Ability, Information Security Behavior

▷ 논문접수 : 2014. 02. 22 ▷ 심사완료 : 2014. 03. 04 ▷ 게재확정 : 2014. 03. 14
* 한국해양대학교 대학원 해운경영학과 박사과정, mswcrash@hanmail.net, 051)410-4384, 대표집필
** 한국해양대학교 해운경영학부 교수, cmhee2004@kmou.ac.kr, 051)410-4384, 교신저자

Ⅰ. 서 론

최근 사상 초유의 고객정보 유출사고를 겪은 금융권이 보안사고가 일어난 이후 정보보호체계를 강화하는 방안을 제시하고 있다. 금융사들은 정보보호 사고가 일어날 때마다 그 해결책으로 임원급 최고정보보호책임자(CISO)선임과 조직의 분리를 내세우고 있다. 조직의 정보보호책임자는 정보기술에 대한 전문지식보다는 실무에서 조직의 통제를 바탕으로 조직의 감사를 진행할 수 있어야 하고, 리더십을 갖춘 임원이 적격자이다. 또한 장기적으로 금융사 정보보호체계를 회계감사처럼 외부 기관으로부터 감사를 받아야 하는 제도의 도입 역시 시급하다는 필요성을 강조한다. 다른 산업에 비해 금융권의 보안수준이 가장 높은데도 불구하고 보안사고가 계속 일어나는 이유에 대해서는 각종 보안 시스템의 한계일 수도 있지만 보안의 가장 큰 위협 요소가 '사람' 이라는 '인적보안' 에서 잠재적인 문제점과 위험이 존재한다는 것이다(보안뉴스, 2014). 인적보안(Personnel Security)이란 조직의 보안정책에 따라 보안임무를 안전하게 수행하는데 영향을 주는 조직구성원들에 관한 보안을 말한다. 조직의 정보자산에 대한 최소 공개의 원칙, 보안인증의 지침 등의 절차 등을 준수할 수 있도록 조직보안에 대한 중요성을 인식시키며, 조직구성원으로부터 보안 문제가 야기되는 것을 방지하기 위한 활동을 말한다.

조직에서 발생하는 보안사고는 사건이 발생한 이후에서야 보안정책을 강조하고 보안대책을 언급한다. 추후 발생할 위험에 대한 논의가 사전에 검토되어야 하며 보안사고를 사전에 방지하는 것이 중요하다(구태언, 2011). 조직에서 사전에 보안점검을 실시하고 조직의 정보보안정책을 수립하여 조직구성원들에게 정보보안에 대한 교육과 훈련이 반복된다면 조직의 정보보안의 문제점을 줄여갈 수 있을 것이다. 보안뉴스(2014)가 발표한 '긴급 7대 보안 수칙' 은 온라인 사이트를 이용할 시 각 사이트별 다른 아이디와 패스워드를 설정하는 것을 권고하고, 아이디와 패스워드는 특수문자를 포함하여 복잡하게 만들기, PC와 휴대폰에 백신프로그램을 설치하고 백신프로그램에 '실시간 감시' 로 설정할 것을 권고하고 있다. 또한 금융계좌 거래 시에는 거래내역 '실시간 알림 서비스' 를 활용하고 공인인증서와 보안카드는 PC와 이메일에 보관하지 않고 별도 보관을 강조하였으며 이메일이나 문자메시지 수신시 모르는 URL은 클릭하지 않는다는 수칙 등이다. 이를 통해 개인정보유출과 바이러스, 악성코드 감염과 각종 피싱(Phishing)과 스미싱(Smishing) 피해를 최소화할 수 있다.

개인의 정보유출이 아닌 조직의 정보유출 즉, 조직정보보안이 구체적으로 이루어지고 있지 않다면 그 피해의 파급효과는 예측하기 어렵다. 조직에서 사전에 조직구성원들로 하여금 조직정보보안에 대한 중요성을 언급하며 이를 위해 해결할 수 있는 방법을 모색하는 것이 조직보안을 위해 반드시 필요로 한다. 전 세계적으로 보안제도를 강화시킨 계기가 된 2001년 미국의 9.11테러 사건 이후 전략물자를 중심으로 정부가 자국의 국가안보와 외교정책, 국내 수급관리를 목적으로 수출입과 공급, 소비 등을 통제하기 위해 각종 보안제도를 도입하고 있다. 특히

해운항만조직의 정보보안은 국가 경쟁력 확보를 위해서도 필수적으로 투자하고 관심을 가져야 하며, 정부와 기업의 대응전략을 수립하여 해운항만조직의 정보보안 방안을 제시할 필요성이 있다. 정보보안관리 시스템을 체계화하여 구축하는 것도 해운물류보안을 위한 중요한 임무이다 (강재영, 2013). 보안제도를 이행하는 조직의 종사자가 반드시 준수해야 하는 정보보안정책의 중요성을 인식시키고 정보보안 능력과 행동을 향상시킴으로서 내부조직의 안전성을 유지할 수 있을 것이다. 해운항만분야에서 정보보안의 중요성이 커지고 있지만 정보보안과 관련된 연구는 부족한 실정이다. 따라서 본 연구에서는 해운항만산업의 정보보안정책이 정보보안능력 및 행동에 어떠한 영향을 미치는 지를 분석함으로써 해운항만분야의 정보보안 상태를 파악할 필요성에 의해서 연구를 수행하였다.

따라서 본 연구의 목적은 해운항만조직 구성원의 정보보안정책 준수 정도가 정보보안 능력과 행동에 미치는 영향요인을 규명하기 위해 실증분석 하는 것이다. 이를 위해서 첫째, 해운항만조직의 정보보안 지침인 정보보안정책 준수 정도를 평가하기 위해 선행요인을 선행연구를 통하여 도출하여 분석한다. 둘째, 해운항만조직 구성원의 정보보안정책 준수 정도와 정보보안 능력 및 행동 간의 관계를 규명하고자 한다.

Ⅱ. 이론적 배경

1. 해운항만조직의 정보보안

조직의 정보보안은 조직의 정보자산이 되는 정보의 완전성을 의미하며 정보의 안정성과 무결성을 지키기 위한 의미로 사용된다. 정보보호는 그 관점을 정보가 아닌 외부의 위협에 초점을 두고 있으며 보안사고를 예방하고 사후보안 해결책에 중점을 두고 있는 개념이다(윤한성, 2007). 즉, 내부의 정보가 외부에 유출되거나 침해되는 것을 막는 것이 조직의 정보보안에 있어 중요하다. 무엇보다 조직에서 보안을 이행할 수 있는 주체가 조직구성원이기에 인적보안의 중요성은 강조되고 있으며 조직구성원이 조직의 보안정책에 따라 보안업무를 안전하게 수행하기 위한 개인적 관점의 업무가 중요하다. 따라서 조직의 정보보안이란 “최소 공개의 원칙, 보안인증의 지침 등의 절차 등을 준수하여 조직구성원으로부터 보안 문제가 야기되는 것을 방지하기 위한 활동” 을 말한다(Halibozek and Kovacich, 2005). 조직 내부 외부의 정보와 정보시스템의 운영, 관리, 활용은 모두 조직의 구성원에 의해 이루어진다는 사실을 감안할 때 정보보안을 위해서 인적 보안은 매우 중요한 위치를 차지한다는 것을 알 수 있다. 직원의 자질이나 능력과 아울러 보안에 영향을 미칠 수 있는 습관이나 배경 등을 면밀하게 판단하여 잠재적인 위협을 미연에 방지하거나 최소화하는 노력이 요구된다. 또한 보안 교육과 관련 정책의 홍보,

보안절차의 훈련 등도 인적 보안 관리에서 이루어져야 할 부분이다. 특히 해운항만조직의 정보보안은 국가 경쟁력 확보를 위해서도 필수적으로 투자하고 관심을 가져야 하며, 정부와 기업의 대응전략을 수립하여 해운항만조직의 정보보안 방안을 제시할 필요성이 있다. 해운항만 조직의 정보보안은 "화물, 선박, 항만시설, 선원 등 해운항만업과 관련된 국가적인 자산을 보호하는 활동" 이다(Hecker, 2004). 해운항만 조직의 선박사고 89%가 운항미숙이나 과실 등 인적요인에 의해 발생하다보니 해양사고예방을 위해 선박운항기술에 정보통신기술(ICT)을 융합한 시스템이 필요하게 되었다. 이에 따라 국제해사기구(IMO)는 해양안전, 보안강화 및 해운물류 효율성 증대를 위해 전략이행계획을 논의하고 있다.

2. 조직의 보안정책 준수와 선행요인

정보보안 정책은 기업이나 조직이 보유하고 정보와 관련성이 높은 영업비밀 및 자산을 다양한 외부 위협으로부터 보호하고, 불법적인 정보기술유출을 사전에 예방하여 기업의 가치 및 자산손실에 대한 피해를 최소화하기 위한 내부의 정책을 문서화 하고 규정한 것이다(노순동, 2004). 기업이나 조직의 내부 업무에 대한 중요 기밀 문서화의 수준이 높을수록 정보보안에 대한 대책방안을 어느 정도 실행해나가는 기업이라고 평가할 수 있다. 일반적으로 기업이나 조직의 보안은 보안정책부분에서 실시되며, 이러한 보안정책은 각 단계별 절차에 따라 문서화하여 규정을 준수할 수 있도록 설계되며 해당 기업의 정보보안 취약점을 지속적으로 분석하고 관리되어야 한다. 보안정책은 기업내부의 보안규정과 보안규칙, 기업의 보안기준에 대한 전반적인 사항들을 강조하며 모든 조직의 구성원들에게 보안정책 원칙사항에 대한 보고와 행동규정에 대해 알려줄 필요성이 있다. Bulgurcu et al.(2010)은 계획된 행동 이론, 합리적 선택 이론과 정보보안 지각을 기반으로 조직원들의 정보보안 정책 준수와 관련된 연구를 하였다. 합리적 선택 이론이란 개인이 선택의 상황에 놓였을 때 어떻게 결정을 내리는지에 대한 설명이다. 즉, 개인이 자신이 생각하는 혜택과 비용을 비교하여 합리적인 부분으로 선택한다고 가정한다. 그리고 이러한 개인의 선호는 선택의 결정의 혜택과 비용에 대한 개인의 인식에 영향을 받는다. 조직원들의 '정보보안 인지' 가 정보보안 정책 준수의 결과에 대한 신념에 영향을 미치고, 이것이 '결과에 대한 종합적 평가에 대한 신념' 에 영향을 미쳐 '태도' 에 영향을 주고, '주관적 신념' 과 '자기 효능감' 과 더불어 '정보보안정책 준수의도' 에 영향을 미치게 된다는 논리이다. 강다연 · 장명희(2012) 연구에서의 정보보안정책 준수에 영향을 미치는 요인들을 실증분석한 결과에 따르면, 해운항만조직 구성원들의 정보보안인식과 정보보안태도와의 관계는 긍정적으로 나타났으며, 정보보안태도와 정보보안정책 준수와의 관계도 긍정적으로 나타났다. 그리고 자기효능감과 정보보안정책 준수와의 관계, 사회적 영향과 정보보안정책 준수의 관계도 긍정적으로 나타났다. Knapp et al.(2006)은 인지된 보안 효과에 영향을 주는 요인으로 사용

자의 훈련, 보안문화, 정책관련성, 정책실행을 밝혀냈다.

본 논문에서의 정보보안정책 준수에 영향을 미치는 선행요인으로 정보보안 규범, 정보보안 처벌, 정보보안 교육으로 선정하였다. 조직의 정보보안규범의 필요성에 대해 언급한 Theoharidou et al.,(2005)는 체계적인 정보보안규범이 정보보안정책준수에 책임을 부여할 수 있는 요인임을 증명하였다. 또한 Berejikian(2002)의 연구에서는 합리적 행동을 결정하기 위한 처벌이 바람직한 행위를 조정한다고 보았다. 안중호 등(2010)은 정보보안을 위한 방안으로 처벌과 윤리교육이 정보보안준수에 영향을 미친다는 것을 정보보안정책과 억제이론의 관점에서 조직유형으로 구분하여 실증분석 하였다.

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. 문현정(2009)은 중소기업의 정보보안을 규모와 성격에 따라 일반 사용자 보안과 기업 보안의 성격을 분석하였으며, 정보보안 역량 강화를 위한 교육 훈련현황에 대한 중요성을 강조하였다.

3. 조직의 정보보안 능력과 선행요인

조직의 정보보안 관리를 위한 능력은 조직종사자들에 의해 정보보안 핵심 요인으로 강조되고 있다. 특히 조직의 정보기술 관련 보안능력, 정보기술 연계능력 등 전략적인 조직보안을 위한 조직종사자들의 보안자세는 정보보안능력을 향상시키는 태도와도 같다. 조직이 정보보안을 위해 종사자들의 지식을 공유하고 정보보안체계를 구축해나가는 것도 정보보안 가능성을 제시해 줄 수 있는 부분이다. 조직의 IT와 비즈니스간의 시너지로 인해 정보보안 관리에 대한 빠르고 효율적인 의사결정이 가능해지고 효율적인 보안관리 전략을 수행이 가능하게 됨으로 인해 조직 내 보안관리 동화가 더 용이해 질 것으로 판단된다. Von Solms(2001)은 조직의 정보자원을 보호하기 위해 정보보안 기술 구현에 많은 투자를 하더라도 조직 구성원이 정보보안에 대한 충분한 인지를 하고 있지 않다면 무용지물이 될 것이라고 했다. 즉, 조직 구성원의 정보보안 중요성에 대한 인식이 전제되지 않은 상태에서 정보보안 기술 자체가 조직의 정보자원을 효과적으로 보호해 줄 수는 없다고 주장하였다. Choi et al.(2008)은 정보보안인식과 정보보안실천 사이의 관계가 직접적으로 유의 하다는 것을 증명하였다. 즉, 정보보안실천에서 중요한 요인은 보안정책과 절차, 보안 훈련 및 교육, 접근제어, 시스템과 프로그램 업데이트, 보안 팀이며, 이는 정보보안인지의 능력과 정보보안수준을 향상시킨다.

4. 조직의 보안행동과 선행요인

Cavusoglu et al.(2009)는 정보보안인식에 따라 조직구성원의 정보보안에 대한 일반적 지식과 조직의 정보보안정책을 준수하기 위한 보안행동이 나타난다고 하였다. 임채호(2006)는 정보보안인식을 조직구성들이 자신의 직무를 수행하는데 있어, 정보보안의 함축된 상태를 잘 알 수 있도록 하는 프로세스라고 정의하였다. 보안행동에 포함되는 요소로 정보보안의 중요성을 인식하고, 보안사고 발생 시 이에 대한 대응방안과 보고체계 등이 필요함을 주장하였다. Siponen & Vance(2000)은 정보보안 행동은 조직에서 정보시스템 사용자와 관련된 실수를 최소화 하고 사용자 관점의 보안 기술 및 절차의 효율성을 최대화 하는 것이라고 주장하였다. Chen et al. (2008)은 기술적 보안 솔루션뿐만 아니라 인간이 정보자산 보호의 중요 요소라고 주장하며 보안행동의 주체를 인간이라고 지적하고 있다. 실제로 보안위협은 사용자의 지식과 행동의 부주의와 결핍에 그 직접적인 원인이 있으므로 오늘날의 정보보안의 성공에 있어 보안행동을 실행할 때 비로소 조직의 보안대책에도 영향을 미칠 것이다. Layton(2005)는 조직구성원의 정보보안행동을 유도하는 요인은 정보보안인식이고 이 인식은 개인의 정보보안에 대한 태도, 동기부여, 도덕, 믿음, 윤리, 개인적 특성간의 연관성에 따른 영향이 있음을 주장하였다.

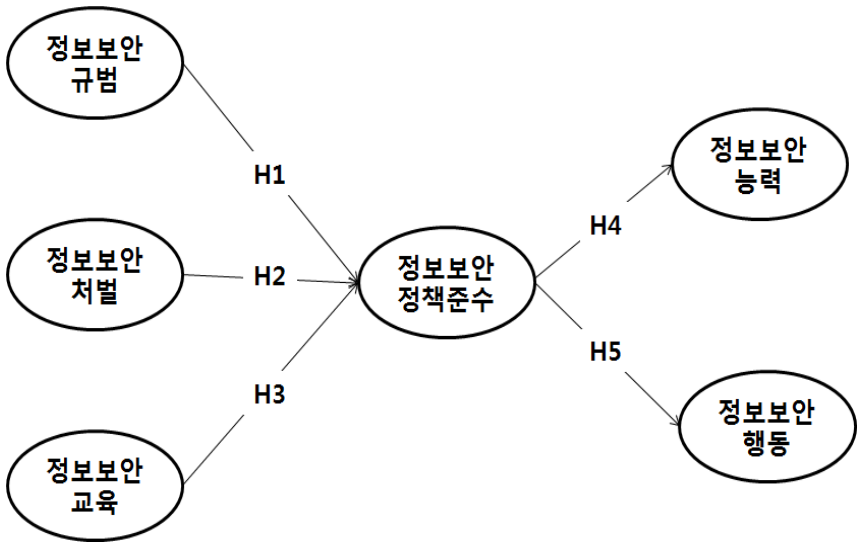
Ⅲ. 연구 설계

1. 연구모형 및 가설설정

본 연구에서는 선행연구에서 논의된 사항들을 토대로 해운항만조직의 정보보안 측면에서 중요한 요인들로 연구모형을 설계하였다. 우선 조직의 정보보안 규범, 정보보안 처벌, 정보보안 교육이 해운항만조직 구성원들의 정보보안정책 준수 정도에 영향을 미치지를 분석한다. 다음으로 해운항만조직 구성원의 정보보안정책 준수 정도가 정보보안능력과 행동에 긍정적인 영향을 미치는지를 확인하고자 〈그림 1〉과 같이 연구모형을 설계하였다.

조직의 정보보안정책은 기업내부의 보안규정과 보안규칙, 기업의 보안기준에 대한 전반적인 사항들을 강조하며 모든 조직의 구성원들에게 보안정책 원칙사항에 대한 보고와 행동규정에 대해 알려줄 필요성이 있다(Bulgurcu et al., 2010). 정보보안정책을 조직의 정보와 기술 자원을 보호하기 위한 조직원들의 역할과 책임감이라고 볼 수 있다. 정보보안정책은 조직의 중요한 정보 및 기술 자원들을 관리, 보호, 배포하는데 필요한 일련의 규칙과 실무지침을 규정해 놓은 것으로 조직 구성원들에게 보안기준을 제시하는 것이다(Lehtinen et al., 2006). 적절한 보안정책준수를 이행할 수 있도록 체계적인 정보보안규범은 반드시 필요하다(Theoharidou et al., 2005). 조직에 규정된 정보보안규범은 임직원 및 정보보안 조직에 대한 각각의 보안임무와

〈그림 1〉 연구모형



와 이에 따른 책임을 부여하기에 정보보안정책 준수를 할 수 있게 된다. Berejikian(2002)의 연구에서는 처벌로 인해 받는 고통을 생각한다면 합리적 행동을 결정하기 위해 행동을 절제한다는 연구결과가 반영되었다. 또한 범죄를 예방하기 위해서는 처벌의 확실성, 엄격성, 신속성을 기반으로 바람직하지 못한 행위를 조정하는 것이 반드시 필요하다(Lebow & Stein, 1990). 정보보안정책 준수에 있어서 긍정적인 효과를 위한 강력한 정보보안처벌은 조직의 정보보안을 위해 정보보안정책을 준수할 수 있는 효과를 가져다 줄 것이다. 정보보안 교육은 조직의 정보보호 업무와 연관된 직원들 및 최종사용자에게 정보보호에 대한 인식을 제고하고, 정보보호대책의 필요성을 이해하도록 하며 구현될 정보보호대책들을 정확하게 사용할 수 있도록 교육 및 훈련 프로그램을 수립하고 이행하여야 한다. 조직의 정보보안을 위해서는 정보보안 교육이 반드시 실시되어야 하며 이는 정보보안정책 준수를 이행하는데 영향력을 가져다준다(Straub, 1990; Workman & Gathegi, 2006). 따라서 정보보안 정책준수 정도에 영향을 미치는 선행요인으로 정보보안규범, 정보보안처벌, 정보보안교육으로 선정하였으며, 다음의 연구가설을 설정하였다.

H1 : 해운항만조직의 정보보안규범은 해운항만조직 구성원의 정보보안정책 준수 정도에 정(+)의 영향을 미친다.

H2 : 해운항만조직의 정보보안처벌은 해운항만조직 구성원의 정보보안정책 준수 정도에 정(+)의 영향을 미친다.

H3 : 해운항만조직의 정보보안교육은 해운항만조직 구성원의 정보보안정책 준수 정도에 정(+)의 영향을 미친다.

정보보안정책 준수는 조직의 정보보안 사항에 대한 이해도를 높이며, 반드시 조직 정보보안을 위해 해결할 수 있는 기술력도 필요하며, 이를 이행하기 위한 정보보안 능력수준이 높아지는데 영향을 미친다(Bulgurcu et al., 2010). 정보보안 능력은 조직의 정보보안을 실천하기 위한 조직구성원들이 정보보안과 관련된 문제점을 해결할 수 있는 능력이기에 보안사고에 대한 대책을 마련하는 방안으로 역량을 키워나가야 한다. 이는 조직의 체계적인 정보보안정책 준수를 하는 정도가 높을 경우 정보보안에 대한 관심과 보안관리를 위한 능력수준이 향상된다는 것으로 볼 수 있다.

정보보안을 실천하기 위한 조직구성원들의 행동도 정보보안정책준수를 이행하였을 때 나타나는 결과라고 볼 수 있다(Pahnila et al., 2007). 정보보안정책에 따라 조직의 업무를 순차적으로 진행하고 발생할 정보보안 사고에 대한 대처방안으로 조직의 정보보안을 위한 실천적인 행동이 나타난다. 따라서 다음과 같은 가설을 도출하였다.

H4 : 해운항만조직 구성원의 정보보안정책 준수 정도는 정보보안 능력에 정(+)의 영향을 미친다.

H5 : 해운항만조직 구성원의 정보보안정책 준수 정도는 정보보안 행동에 정(+)의 영향을 미친다.

2. 연구변수의 조작적 정의 및 항목

본 연구에서는 해운항만조직의 정보보안정책준수 정도가 해운항만조직 구성원의 정보보안 능력과 정보보안 행동에 영향을 미치는 요인을 검정하기 위해 연구 개념들은 아래의 〈표 1〉과 같이 조작적으로 정의하였으며, 모든 측정항목은 리커트(Likert) 7점 척도로 설문항목을 구성하였다.

〈표 1〉 연구변수의 조작적 정의 및 항목

연구 요인	조작적 정의	설문항목	참고문헌
정보 보안 규범	조직 내 정보보안을 위해 규정된 정보보안 규범을 조직 구성원이 정보보안에 긍정적이라 생각하는 정도	• 정보보안규범의 안전성 • 정보보안규범의 신뢰성 • 정보보안규범의 우수성 • 정보보안규범의 업무보안성	Soponen & Vance(2010) Piquero et al.(2005) Siponen(2000)
정보 보안 처벌	조직 내 정보보안 규범을 준수하지 않을 경우 조직구성원에게 돌아오는 불이익이 가해질 수 있는 정도	• 상위관리자의 통보 처벌 • 시스템 사용 제한의 처벌 • 불이익에 대한 처벌 • 업무활동 제한의 처벌	Workman & Gathegi(2006) Kurland(2006) Berejikian(2002)
정보 보안 교육	조직의 정보보안교육에 대한 조직구성원들의 인지된 효용성	• 정보보안교육의 유익성 • 정보보안교육의 적합성 • 정보보안교육의 활동성 • 정보보안교육의 적용성	Workman & Gathegi(2006) Layton(2005) Knapp et al.(2005) 백민정 & 손승희(2010) 안중호 등(2010) 이선중 & 이미정(2008)
정보 보안 정책 준수	조직의 정보보안과 관련된 정책, 가이드라인을 준수할 때 정보보안활동에 도움을 주는 정도	• 업무보안의 적용성 • 보안활동 행동의 유용성 • 보안확인의 유용성 • 보안활동의 효과성	Bulgurcu et al.(2010) Halibozek & Kovacich(2005) Siponen(2000)
정보 보안 능력	조직의 정보보안 사항에 대해 이해하며 해결할 수 있고 정보보안기술을 적용할 수 있는 능력의 정도	• 정보보안 피해 인식도 • 정보보안 기술 사용방법 • 정보보안 기술 활용도 • 정보보안 문제해결 능력	Bulgurcu et al.(2010) Gist(1987) Bandura(1977)
정보 보안 행동	조직의 정보보안을 실행하기 위한 조직구성원들의 실천적인 행동사항의 정도	• 주기적인 패스워드 변경 • 정보보호 실천 • 업무문서 파기 • 출처가 명확한 파일 다운로드	Pahnila et al.(2007) Kurland(2006) Lee et al.(2004)

정보보안 규범의 조작적 정의는 조직 내 정보보안을 위해 규정된 정보보안 규범을 조직구성원이 정보보안에 긍정적이라 생각하는 정도라고 정하였으며, 측정항목으로는 정보보안 규범의 안전성, 정보보안 규범의 신뢰성, 정보보안 규범의 우수성, 정보보안 규범의 업무보안 안전성

을 선정하였다. 정보보안 처벌은 조직 내 정보보안 규범을 준수하지 않을 경우 조직구성원에게 돌아오는 불이익이 가해질 수 있는 정도라고 조작적 정의를 내렸으며, 측정항목으로 상위관리자의 통보 처벌, 시스템 사용 제한의 처벌, 불이익에 대한 처벌, 업무활동 제한의 처벌로 구성하였다. 정보보안 교육은 조직의 정보보안교육에 대한 조직구성원들의 인지된 효용성이라고 조작적 정의를 하였으며, 측정항목으로 정보보안 교육의 유익성, 정보보안 교육의 적합성, 정보보안 교육의 활동성, 정보보안 교육의 조직업무 적용성으로 선정하였다. 또한 정보보안정책 준수의 조작적 정의는 조직의 정보보안과 관련된 정책, 가이드라인을 준수할 때 정보보안활동에 도움을 주는 사항의 정도라고 정하였다. 측정항목으로 보안정책기반 업무보안의 적용성, 보안정책기반 보안활동 행동의 유용성, 보안정책기반 보안확인의 유용성, 보안정책기반 보안활동의 효과성으로 선정하였다.

정보보안능력 수준은 조직의 정보보안 사항에 대해 이해하며 해결할 수 있고 정보보안기술을 적용할 수 있는 능력의 정도라고 조작적 정의를 내렸으며, 정보보안 피해 인식도, 정보보안 기술 사용방법, 정보보안 기술 활용도, 정보보안 문제해결능력으로 평가하고자 구성하였다. 정보보안행동의 조작적 정의는 조직의 정보보안을 실행하기 위한 조직구성원들의 실천적인 행동사항 정도라고 정하였으며, 이를 측정하기 위한 항목으로 주기적인 패스워드 변경, 정보보호 실천행동, 조직의 정보보안을 위한 업무문서 파기, 출처가 명확한 파일을 확인한 후 다운로드하는 항목으로 선정하였다.

Ⅳ. 실증분석

1. 분석기법 및 표본의 특성

본 연구에서는 해운항만조직 구성원의 정보보안정책 준수정도가 정보보안능력과 정보보안행동에 어떠한 영향을 미치는지 평가하기 위해 현재 해운항만 조직에 재직 중인 종사자들을 표본집단으로 선정하여 설문을 수행하였다. 연구모형의 분석을 위해 전체 170부의 설문을 배포하여 158를 회수하였으며, 결측치가 있거나 불성실하게 응답한 4부의 설문지를 제외한 총 154부를 최종분석에 활용하였다. 수집된 데이터는 응답자의 인구통계학적특성 분석을 위해 SPSS Windows 15.0이 사용되었으며, 연구모형의 적합성을 검증하기 위해 적용된 구조방정식 모델의 평가를 위해 AMOS 7.0으로 분석하였다.

〈표 2〉 인구통계학 특성 분석

구분	항목	빈도수	비율(%)
성별	남자	122	79.2
	여자	32	20.8
연령	20~30세 미만	22	14.3
	30~40세 미만	71	46.1
	40~50세 미만	49	31.8
	50세 이상	12	7.8
해운/항만업 조직유형	선사 및 포워딩사	92	59.7
	터미널 및 운영사	42	27.3
	종합물류기업	6	3.9
	물류정보기술 관련기업	5	3.3
	기타(공사)	9	5.8
직급	사원	24	15.6
	대리	50	32.5
	과장	51	33.1
	부장	27	17.5
	이사	2	1.3
종업원 수	100명 이하	17	11
	300명 이하	51	33.1
	500명 이하	54	35.1
	1000명 이하	25	16.2
	1000명 이상	7	4.5
연간매출액	50억 미만	16	10.4
	200억 미만	15	9.7
	500억 미만	30	19.5
	500억 이상	93	60.4
합계		154	100

〈표 2〉에서 보는 바와 같이 응답자의 표본특성을 살펴보면 남자가 122명(79.2%), 여자가 32명(20.8%)으로 나타났으며, 연령대는 30~40대가 71명(46.1%)으로 가장 높게 나타났으며, 다음으로 40~50대가 49명(31.8%)를 차지하였다. 해운/항만업의 조직유형으로 선사 및 포워딩사가 92명(59.7%), 터미널 및 운영사가 42명(27.3%) 기타(공사)가 9명(5.8%), 종합물류기업이 6명(3.9%), 물류정보기술 관련기업이 5명(3.3%)순으로 나타났다. 직급은 과장 51명(33.1%),

대리 50명(32.5%), 부장 27명(17.5%), 사원24명(15.6%), 이사 2명(1.3%)를 차지하였다. 종업원 수는 500명 이하가 54명(35.1%)로 가장 빈도가 높게 나타났으며 다음으로 300명 이하가 51명(33.1%)로 나타났으며 연간매출액은 500억 이상이 93명(60.4%), 500억 미만 30명(19.5), 50억 미만 16명(10.4%), 200억 미만 15명(9.7%) 순으로 확인할 수 있다.

본 연구의 응답자가 속한 조직보안 관련 특성은 다음의 〈표 3〉과 같다. 보안전담조직 있음이 116명(75.%), 없음이 38명(24.7)로 나타났으며, 보안정책이 있음이 142명(92.2%), 없음이 12명(7.8%)로 확인되었다. 조직의 보안정책 미준수시 불이익을 받게 되는 보안처벌은 있음이 115명(74.7%), 없음이 39명(25.3%)로 분석되었다. 그리고 조직의 연간 보안교육 횟수는 1회가 66명(42.9%)로 가장 높게 나타났으며 2~3회가 56명(36.4%), 4~5회가 19명(12.3%), 6회 이상이 13명(8.4) 순으로 나타났다.

〈표 3〉 응답자의 조직보안 관련 특성

구분		빈도(명)	비율(%)
보안전담조직	있음	116	75.3
	없음	38	24.7
보안정책	있음	142	92.2
	없음	12	7.8
보안처벌	있음	115	74.7
	없음	39	25.3
연간 보안교육	1회	66	42.9
	2~3회	56	36.4
	4~5회	19	12.3
	6회 이상	13	8.4
합계		154	100

2. 측정모형의 신뢰성과 집중타당성

본 연구에서는 확인적 요인분석을 통해 측정모형의 내적신뢰성을 평가하기 위한 합성개념 신뢰도와 평균분산추출 값(AVE), Cronbach-α값을 분석하였으며 결과는 〈표 4〉에 제시하였다.

〈표 4〉 집중타탕성과 신뢰성 분석

요인	항목	집중타당성				내적신뢰성		
		비표준화 추정치	표준화 추정치	t-값	측정 오차	합성 개념 신뢰도	AVE	cronbach-α
정보보안규범 (SS)	SS1	0.996	0.899	19.98	0.101	0.977	0.913	0.92
	SS2	0.986	0.943	23.791	0.057			
	SS3	1	0.945	-	0.055			
	SS4	0.938	0.891	19.407	0.109			
정보보안처벌 (SP)	SP1	0.658	0.636	9.022	0.364	0.921	0.748	0.787
	SP2	0.888	0.829	14.045	0.171			
	SP3	0.761	0.735	11.41	0.265			
	SP4	1	0.947	-	0.053			
정보보안교육 (SE)	SE1	0.838	0.877	17.359	0.123	0.967	0.879	0.891
	SE2	0.906	0.885	17.791	0.115			
	SE3	1	0.927	-	0.073			
	SE4	0.904	0.875	17.246	0.125			
정보보안정책 (POL)	POL1	0.917	0.884	17.794	0.116	0.948	0.823	0.845
	POL2	1	0.936	-	0.064			
	POL3	0.871	0.86	16.598	0.14			
	POL4	0.844	0.698	10.869	0.302			
정보보안능력 (SA)	SA1	0.727	0.663	9.068	0.337	0.893	0.685	0.739
	SA2	1	0.871	-	0.129			
	SA3	0.984	0.886	13.449	0.114			
	SA4	0.846	0.536	6.928	0.464			
정보보안행동 (SB)	SB1	0.96	0.589	6.55	0.411	0.801	0.507	0.62
	SB2	0.553	0.519	5.736	0.481			
	SB3	0.78	0.62	6.853	0.38			
	SB4	1	0.75	-	0.25			

우선, 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 나타났으며 정보보안 규범, 정보보안 처벌, 정보보안 교육, 정보보안정책 은 모두 0.9 이상으로 높게 평가되었다. 평균분산추출 값(AVE) 결과도 권장수준0.5이상을 상회하였기에 모두 양호한 결과로 확인하였다. 내적신뢰도에서 Cronbach-α값이 권장기준 0.7이상의 수용기준에 부합되어야 하는데 정보보안행동이 0.62로 조금 낮게 측정되었지만 합성개념 신뢰도와 AVE값이 충분히 충족되기에 내적신뢰성이 확보되

었음을 알 수 있다.

집중타당성 결과를 살펴보면 측정항목의 추정치가 0.5이상이며, 그 추정치의 t-값이 2.0 이상일 때, 측정항목의 집중타당성이 있는 것으로 판단한다. 〈표 4〉에 나타나 있듯이 모든 항목들의 추정치와 그 추정치의 t-값은 권고되는 수치를 충분히 만족시키는 것으로 나타나 연구에 적용된 항목들의 집중타당성은 충분히 있다고 판단할 수 있다.

3. 측정모형의 판별타당성

본 연구에서의 판별타당성 결과는 〈표 5〉에서 보는 바와 같다. 각 구성개념들의 평균분산추출 값(AVE)의 제곱근이 다른 구성개념들 간의 상관계수 값보다 상회하고 있어 변수간의 판별타당성이 있음을 확인할 수 있다. 구성개념 내의 평균분산추출 값이 다른 구성개념과 공유하는 분산보다 크다는 것으로 변수간의 판별타당성을 측정하였다.

〈표 5〉 변수 간 상관계수와 AVE의 제곱근 값

변수	추출된 평균분산의 제곱근 값					
	1	2	3	4	5	6
1. 정보보안 규범	(0.956)					
2. 정보보안 처벌	0.58	(0.865)				
3. 정보보안 교육	0.646	0.733	(0.938)			
4. 정보보안 정책준수	0.737	0.55	0.800	(0.907)		
5. 정보보안 능력수준	0.403	0.399	0.663	0.603	(0.828)	
6. 정보보안 행동	0.582	0.603	0.683	0.729	0.723	(0.801)

주 : ( )는 각 변수의 AVE 제곱근.

4. 측정모형과 구조모형의 적합도 평가

본 연구의 측정모형과 구조모형에 대한 적합도 지수는 아래의 〈표 6〉과 같다. 먼저측정모형을 살펴보면 χ^2(p)은 401.076(0.00)이며, χ^2을 자유도로 나눈 비율이 1.707로 권장수준(≤ 3.00)에 부합하였다. 구조모형에서도 χ^2(p)은 432.098(0.00)이며, χ^2을 자유도로 나눈 비율이 1.793으로 권장수준(≤3.00)에 부합하였다. GFI는 측정모형이 0.819, 구조모형이 0.812로 권장수준인 0.90보다 약간 낮게 분석되었지만 AGFI가 0.80에 근접하고 있으며, RMSEA 값은 측정모형과 구조모형 모두가 수용기준에 부합하는 것으로 나타났다. 또한 IFI, CFI가 각각 측

정모형이 0.947, 구조모형이0.938이며, PGFI가 측정모형0.641, 구조모형 0.652로 나타났으며 PNFI가 측정모형 0.749, 구조모형 0.760로 수용기준을 상회하는 것으로 나타나 대체적으로 측정모형의 적합도가 수용기준을 충족하는 것으로 평가하였다. 또한 구조모형 적합도 역시 연구 개념들 사이의 관계를 설명하는데 적절한 것으로 판단하였다.

〈표 6〉 적합도 지수

구분	적합도 지수	수용기준	측정모형 분석결과	구조모형 분석결과
절대 부합 지수	χ^2/df	≤3.00	1.707	1.793
	χ^2 자유도(df) p-value	≥0.05	401.076 235 0.00	432.098 241 0.00
	기초부합지수(GFI)	≥0.90	0.819	0.812
	근사원소평균자승잔차(RMSEA)	≤0.08	0.068	0.072
증분 부합 지수	수정부합지수(AGFI)	≥0.80	0.769	0.760
	표준부합지수(NFI)	≥0.90	0.880	0.871
	관계부합지수(RFI)	1.0근사	0.859	0.852
	증분부합지수(IFI)	1.0근사	0.947	0.938
	비교부합지수(CFI)	≥0.90	0.946	0.938
간명 부합 지수	간명기초부합지수(PGFI)	≥0.60	0.641	0.652
	간명표준부합지수(PNFI)	≥0.60	0.749	0.760

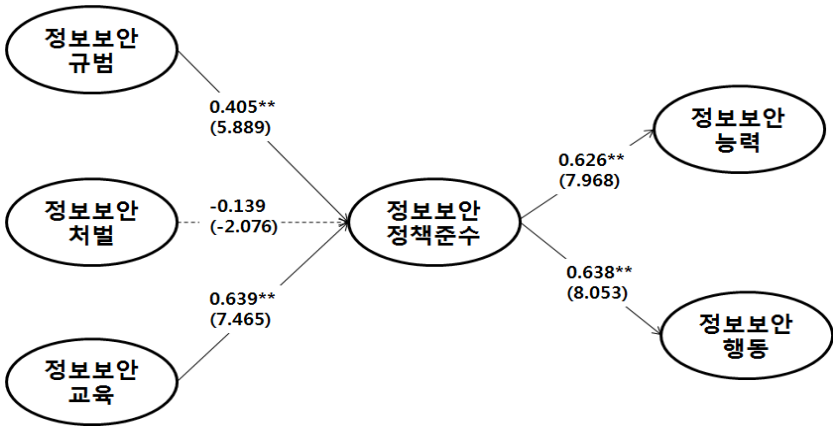
5. 가설검정 및 결과분석

구조모형의 분석결과에 따라 각 경로의 추정치와 t-값은 아래의 〈그림 2〉와 같이 나타났으며, 정보보안처벌이 정보보안정책준수 정도에 이르는 경로를 제외한 다른 모든 경로는 통계적으로 유의한 것으로 확인되었다.

정보보안규범이 정보보안정책준수에 미치는 영향을 평가하기 위해 설정한 연구가설1(H1)은 경로계수가 0.405로 나타났으며, t-값이 5.889로 유의수준 p〈0.01에서 통계적으로 유의한 것으로 나타나 가설이 채택되었으며 , 정보보안교육이 정보보안정책 준수에 미치는 영향을 평가하기 위한 연구가설3(H3)도 경로계수가 0.639이며, t-값이 7.465로 유의수준 p〈0.01에서 통계적으로 유의한 것으로 나타나 채택되었다. 하지만 정보보안 정책준수에 영향을 미치는 가설

2(H2)인 정보보안처벌 선행요인은 경로계수가 -0.139, t-값이 -2.076으로 통계적으로 유의하지 못한 결과를 미쳐 연구가설이 기각되었다. 정보보안정책준수가 정보보안 능력수준에 영향을 미친다는 연구가설4(H4)는 경로계수가 0.626, t-값이 7.968로 유의수준 p<0.01에서 통계적으로 유의한 값을 보여 가설이 채택되었으며, 정보보안정책 준수가 정보보안행동에 영향을 미친다는 마지막 가설5(H5)도 경로계수가 0.638이며, t-값이 8.05, 유의수준 p<0.01에서 통계적으로 유의한 결과를 나타내어 연구가설을 채택하였다. 연구가설 검증결과는 아래의 <표 7>과 같다.

<그림 2> 연구모형 검증결과



주) **:p<.01 에서 유의함

<표 7> 연구가설 검증결과 요약

연구가설	경로 계수	t-값	검정결과
[H1] 정보보안규범은 정보보안정책 준수에 정(+)의 영향을 미친다.	0.405	5.889**	채택
[H2] 정보보안처벌은 정보보안정책 준수에 정(+)의 영향을 미친다.	-0.139	-2.076	기각
[H3] 정보보안교육은 정보보안정책 준수에 정(+)의 영향을 미친다.	0.639	7.465**	채택
[H4] 정보보안정책 준수는 정보보안 능력수준에 정(+)의 영향을 미친다.	0.626	7.969**	채택
[H5] 정보보안정책 준수는 정보보안 행동에 정(+)의 영향을 미친다.	0.638	8.053**	채택

Ⅴ. 결 론

조직에서 발생하는 정보보안 사고는 매해 증가하는 추세이며 그로 인한 정보보안 위험성은 높아져가고 있다(Anderson & Agarwal, 2010). 개인적 측면의 정보보안 관리가 곧 기업의 정보보안에 영향을 미치게 되며 이는 조직외부보다 조직내부의 손실에 크게 작용할 위험성을 가지고 있다고 볼 수 있다. 조직의 정보보안의 내부 위협으로부터 발생한 피해는 경제적 손실뿐만 아닌 사회적인 손실을 가져다준다. 이러한 정보보안의 사고를 방지하기 위해 기업 내부의 성공적인 보안 관리를 위한 정보보안 가이드라인인 조직의 정보보안정책 준수의 강화를 강조할 필요성이 있으며, 정보보안 정책을 잘 준수하기 위한 방안을 모색해야한다.

따라서 본 연구에서는 조직의 정보보안을 위한 해운항만 종사자의 정보보안정책준수 정도에 영향을 미치는 선행요인을 파악하며, 이를 통한 정보보안정책준수 정도가 조직의 정보보안을 위한 종사자의 정보보안능력과 정보보안행동에 긍정적인 영향을 미치는지 연구모형을 설계하여 실증분석을 하였다.

본 연구결과를 요약하면 다음과 같다. 첫째, 해운항만 조직의 정보보안정책 준수에 영향을 미치는 요인으로 정보보안규범과 정보보안교육으로 분석되었다. 우선 정보보안규범이 정보보안정책 준수에 영향을 미친다는 가설1(H1)은 경로계수가 0.405로 나타났으며, t-값이 5.889로 유의수준 P〈0.01에서 통계적으로 유의한 결과를 나타내었다. 정보보안교육이 정보보안정책준수에 영향을 미친다는 가설3(H3)은 경로계수가 0.639, t-값이 7.465로 유의수준 P〈0.01에서 통계적으로 유의한 결과를 나타내었다. 이는 조직 내 규정된 정보보안 규범이 조직구성원이 생각하기에 조직보안에 도움을 주며, 조직의 정보보안교육이 효과적이라고 생각하기에 정보보안정책 준수에 영향을 미치는 결과로 볼 수 있다.

둘째, 조직의 정보보안 처벌은 조직의 정보보안정책 준수 정도에 유의한 영향을 미친다는 가설2(H2)는 경로계수가-0.139, t-값이 -2.076으로 분석되어 통계적으로 유의하지 않은 결과가 도출되었다. 이와 같은 결과는 정보보안정책에 포함된 지침과 가이드라인을 준수하지 않았을 때 처벌하는 부정적인 요인보다는 정보보안정책을 준수할 수 있도록 보상적인 측면을 강화시키는 방안을 모색할 필요성을 제기하고 있다.

셋째, 조직의 정보보안정책 준수는 조직보안을 위한 조직구성원들의 정보보안능력과 정보보안행동에 긍정적인 영향을 미치는 결과를 나타내었다. 먼저 정보보안정책 준수는 정보보보안능력에 영향을 미친다는 가설4(H4)는 경로계수가 0.626, t-값이 7.969로 유의수준 p,0.01에서 통계적으로 유의한 결과를 나타내었다. 또한 정보보안정책 준수가 정보보안행동에 영향을 미친다는 가설5(H5)도 경로계수가 0.638 t-값이 8.053으로 유의수준 p,0.01에서 통계적으로 유의한 결과가 분석되었다. 조직구성원들의 정보보안 능력향상과 정보보안행동을 실천적으로 행할 수 있도록 하는 조직의 정보보안정책이 마련되어 있을 때, 조직의 정보보안을 위한 성과

적인 측면을 기대할 수 있을 것이다.

본 연구의 의의는 해운항만 조직의 정보보안을 위한 정보보안정책 준수를 위해 실제 적용하고 강조해야 하는 선행요인을 도출하였다는 점이다. 정보보안 규정과 정보보안 교육의 중요성을 확인할 수 있었으며, 정보보안정책이 준수되지 않았을 경우에 처벌하는 부정적인 측면보다는 정보보안정책을 준수할 경우에 돌아가게 되는 보상의 중요성을 인식할 수 있었다. 따라서 해운항만조직 구성원의 정보보안정책 준수 정도를 높이기 위해서는 긍정적인 보상체계가 마련되어야 할 것이다.

향후 연구에서는 보안전담조직이 있는 해운항만 조직과 보안전담조직이 없는 해운항만 조직의 정보보안 능력수준과 정보보안 행동을 비교、분석하는 연구가 진행되어야 할 것이다.

참고문헌

강다연 · 장명희, “해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인”, 『한국항만경제학회지』, 제28권 제1호, 2012, 1-23.

강재영, “항만물류보안관리 시스템의 체계화와 일원화 방안”, 『법과 정책연구』, 제13권 제2호, 2013, 389-436.

구태언, “기업의 순환계 IT System과 정보보안의 중요 이슈”, DIGIECO Focus, 2011.

노순동, “기업체의 효율적인 보안관리 모델”, 『산업보안논총』, 창간호, 2004, 79-101.

문현정, “우리나라 중소기업의 정보 보호 역량 강화를 위한 교육 훈련 현황과 문제점”, 『정보보호학회지』, 제19권 제1호, 2009, 29-39.

백민정 · 송승희 “조직의 정보윤리실천이 구성원의 정보보안인식과 행동에 미치는 영향에 관한 연구”, 『경상논총』, 제28권 제4호 2010, 119-145.

보안뉴스, 카드사 개인정보 유출사고 문제점 5가지, 2014. 2. 21.

보안뉴스, 개인정보유출 막는 ‘긴급7대보안수칙’ 발표, 2012, 2. 20.

안중호 · 박준형 · 성기문 · 이재홍, “처벌과 윤리 교육 이정보 보안 준수에 미치는 영향: 조직유형의 조절효과를 중심으로”, 『Information Systems Review』, 제2권 제호 2010, pp.23-42.

윤한성, “정보보안 및 정보시스템자산 관리를 위한 내부 감시, 통제시스템”, 『Information Systems Review』, 제9권, 제1호, 2007, 121-137.

이선중 · 이미정, “정보보호문화의 평가지표에 관한 탐색적 연구”, 『정보화정책』, 제15권 제3호, 2008, 100-119.

임채호, “효과적인 정보보호인식제고 방안”, 『정보보호학회지』, 제16권 제2호, 2006, 30-36.

Berejikian, J., “A Cognitive Theory of Deterrence,” *Journal of Peace Research*, Vol.39, 2002, 165-183.

Bandura, A., Self-Efficacy: The Exercise of Control. New York: W. H. Freeman, 1977.

Bulgurcu, B., Cavusoglu, H. and Benbasat I., “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *MIS Quarterly*, Vol.34, No.3, 2010, 523-548.

Cavusoglu, H. and Son, J., Information Security Control Resources in Organization: A Multidimensional View and Their Key Drivers, 2009.

Chen, C., Medlin, B. and Shaw, R., “A Cross-Cultural Investigation of Situational Information Security Awareness Programs,” *Information Management and Computer Security*, Vol.16, No4, 2008, 360-376.

Choi, N., Kim, D., and Whitmore, A., “Knowing is Doing,” *Information Management and Computer Security*, Vol.16, No.5, 2008, 484-501.

Gist, M. E., "Self-efficacy: Implications for Organizational Behavior and Human Resource Management," *Academy of Management Review*, Vol.12, 1987, 472-485.

Goodhue, D. and Straub, D., "Security Concerns of System User: A Study of Perceptions of the Adequacy of Security," *Information and Management*, Vol.20, No.1, 1991, 13-27.

Halibozek, E., and Kovacich, G., "Mergers and Acquisitions Security: Corporate Restructuring and Security Management," Burlington MA: Elsevier Butterworth-Heinemann, 2005. 57.

Hecker, J. Z., "Port Security: Nation Faces Formidable Challenges in Marking New Initiatives Successful", U. S. General Accounting Office, August 1, 2002 ; Harrald, J. R., et al., "A Framework for Sustainable Port Security," *Journal of Homeland Security and Emergency Management*, Vol.1, No.2, 2004, 1-13.

Knapp, K., Marshall, T., Rainer, R., and Ford, F., "Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness. White Paper," *Information Systems Security Certification Consortium (ISC)*, Vol.2. 2005.

Kurland, N., "Ethical Intentions and the Theories of Reasoned Action and Planned Behavior1," *Journal of Applied Social Psychology* , Vol.25, No.4, 2006, 297-313.

Layton, T., Information Security Awareness: The Psychology Behind the Technology, Author House. 2005.

Lebow, R. and Stein, J., "Deterrence: The Elusive Dependent Variable," *World Politics: A Quarterly Journal of International Relations*, Vol.42, No.3, 1990, pp. 336-369.

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

Nosworthy, J., "Implementing Information Security in the 21 super(st) Century-do You have the Balancing Factors?," *Computer and Security*, Vol.19, No.4, 2000, 337-347.

Pahnila S., Siponen, M., Mahmood, A., "Employees' Behavior towards IS Security Policy Compliance," *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, January 03-06, 2007, p.156.

Piquero, N. L., Tibbetts, S. G. and Blankenship, M. B., "Examining the Role of Differential Association and Techniques of Neutralization in Explaining Corporate Crime," *Deviant Behavior*, Vol.26, No.2, 2005, 159-188.

Rogers, E. M., Diffusion of Innovations. 3rd ed., New York: The Free Press. 1983.

Straub, D. and Welke, R., "Coping with Systems Risk: Security Planning Models for

Management Decision Making," *MIS Quarterly*, Vol.22, No.4, 1998, 441-469.

Siponen and Vance. M., "A Conceptual Foundation for Organization Information Security Awareness, Information," *Management and Computer Security*, Vol.8, No.1, 2000, 31-41.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E., "The Insider Threat to Information Systems and The Effectiveness of ISO17799," Computers and Security, Vol.24, 2005, 472-484.

Solms, B., "Information Security-A Multidimensional Discipline," *Computer and Security*, Vol.20, No.6, 2001, 504-508

Workman, M., and Gathegi, J., "Punishment and Ethics Deterrents: A Study of Insider Security Contravention," *Journal of the American Society for Information Science and Technology*, Vol.58, No.2, 2006, 212-222.

한국항만경제학회지 2014 제30집 제1호, 97-118.

국문요약

정보보안정책 준수가 정보보안능력 및 행동에 미치는 영향 분석 : 해운항만조직구성원을 대상으로

강다연 · 장명희

최근 발생한 고객정보유출사고는 조직의 정보보안 강화에 대한 관심과 전담조직의 중요성을 고조시키고 있다. 이에 따라 기업들은 정보보안 강화를 위해 정보보안정책을 마련하고 있으며, 조직구성원들로 하여금 보안정책을 준수하도록 권고하고 있다. 해운항만 조직에서도 정보보안을 위해 정보보안정책을 체계화시키고 조직구성원들의 정보보안능력과 정보보안행동을 평가할 필요성이 있다. 본 연구의 목적은 해운항만조직 구성원들을 대상으로 정보보안정책 준수 정도가 정보보안능력과 정보보안행동에 미치는 영향을 분석하는데 있다. 분석결과, 먼저 해운항만조직 구성원의 정보보안정책 준수에 영향을 미치는 요인으로 정보보안규범과 정보보안교육을 확인할 수 있었고, 정보보안처벌은 정보보안정책 준수에 유의한 영향을 미치지 않는 것으로 분석되었다. 해운항만조직 구성원의 정보보안정책 준수정도는 정보보안능력과 정보보안행동에 유의한 영향을 미치는 결과를 확인할 수 있었다.

핵심 주제어 : 해운항만조직, 정보유출, 정보보안정책 준수, 정보보안능력, 정보보안행동