한국항해항만학회지 제36권 제3호(Vol. 36, No. 3), pp. 261~271, 2012 (ISSN-1598-5725/eISSN-2093-8470)
Journal of Navigation and Port Research
DOI : http://dx.doi.org/10.5394/KINPR.2012.36.3.261

항만기업 종사자들의 정보보안인식과 지각된 정보보안위험에 영향을 미치는 요인

장명희* · 강다연**

* 한국해양대학교 해운경영학부 부교수, ** 한국해양대학교 대학원 해운경영학과

Factors Affecting the Information Security Awareness and Perceived Information Security Risk of Employees of Port Companies

Myung-Hee Chang · Da-Yeon Kang***

** Division of Shipping Management, Korea Maritime University, Busan 606-791, Korea*
*** Department of Shipping Management, Graduate School of Korea Maritime University, Busan 606-791, Korea*

요 약 : 본 연구의 목적은 항만기업 종사자들의 정보보안인식정도와 지각된 정보보안위험 정도에 영향을 미치는 요인들이 어떤 것들이 있는지를 실증 분석하는 것이다. 특히, 지각된 정보보안위험에 영향을 미치는 요인을 파악하기 위하여 위험분석방법론을 토대로 자산, 위협, 취약성과의 관계를 분석하였다. 252개의 유효설문을 대상으로 AMOS를 이용한 구조방정식 모형 분석을 하였다. 연구결과를 보면, 첫째, 항만기업 종사자의 경우 정보자산은 지각된 정보보안위험에 유의하지 않은 결과로 분석되었다. 둘째, 위협, 취약성은 지각된 정보보안위험에 유의한 영향을 미치는 것으로 나타났다. 마지막으로, 정보보안인식과 정보보안교육, 정보보안인식과 정보보안의도와의 관계는 유의하게 분석되었다. 그러나 정보보안관심도는 정보보안인식에 유의하지 않은 것으로 분석되었다.

핵심용어 : 항만기업 종사자, 정보보안인식, 지각된 정보보안위험, 정보보안의도, 위협, 취약성

Abstract : *The purpose of the present study is to empirically examine factors that affect the information security awareness and perceived information security risk of employees of port companies. In particular, in order to identify factors that affect the perceived information security risks, we investigated the relation of assets, threats, and vulnerabilities to it, using the risk analysis methodology. With A total of 252 valid questionnaires, we also performed the structural equation modeling analysis using AMOS. It was found that first, there was no meaningful relationship between the information assets and the perceived information security risk in the case of employees of port companies. Second, threats and vulnerabilities turned out to have positive influences on the perceived information security risk. Finally, there was a positive relationship not only between the information security awareness and the information security education, but also between the information security awareness and the intention of information security. However, there was no meaningful relationship between the information security concern and the information security awareness.*

Key words : *Employee of Port Companies, Information Security Awareness, Perceived Information Security Risk, Information Security Intention, Threat, Vulnerabilities*

1. 서 론

정보화 정책의 지속적인 추진 결과 현재 최고의 정보화 인프라를 구축하여 IT강국으로 성장하였다. 2010 국가정보보호백서에 따르면 우리나라 인터넷 이용현황에서 2009년 인터넷 이용자가 3,658만 명으로 77.2%를 차지하였으며, 연령대는 10대에서 30대 국민 중 99%가 인터넷을 이용하고 어린이와 40대의 인터넷 이용률도 80%달하는 등 세계 최고 수준의 정보통신 인프라를 확충하고 정보화 선진사회로 진입하였다(정보통신부, 2010). 하지만 정보화의 비약적인 발전과 함께 정보화 사회의 역기능인 개인정보 유출, 피싱(Phishing), 파밍(Pharming), 스팸메일 등으로 인한 개인적인 피해가 증가하고 개인정보를 도용한 사생활 침해와 같은 부작용이 심각한 사회문제로 대두되었다.

특히, 조직에서는 정보보안사고의 가장 큰 위험이 조직 구성원의 정보보안의식 결여로부터 비롯된다. 통계적으로 정보보안을 해치는 주요 요인 중 가장 높은 비율을 차지하는 것이 기업 구성원들의 낮은 보안의식 또는 보안상의 실수로 인한 경우이다. 조직에서는 정보보안의 중요성은 언급하고 있지만 조직구성원 개개인의 보안태도가 호의적 혹은 비호의적이라고 평가할 수 있는 기준이 명확하지 않다. 조직에서 체계적인 정보보안 목표를 효율적이고 효과적으로 달성하기 위해서는 조직 구성원들

* 대표저자 : 종신회원, cmhee2004@hhu.ac.kr 051)410-4384
** 연회원, mswcrash@hanmail.net 010)2968-8529

의 정보보안 인식수준을 정확히 평가하고 이를 개선시킬 수 있는 방향을 제시하는 기준이나 평가모델이 필요하다. 정보보안(Information Security)이란 발생 가능한 모든 정보유출 및 다양한 위협으로부터 기업의 가치 있는 정보를 보호하며, 회사의 기업비밀 및 정보자산이 관계자 외 또는 타 경쟁기업에 공개 혹은 유출되지 않도록 하는 유형, 무형의 모든 예방조치이며 위험 상황 발생 시에 기업의 피해를 최소화하여 업무의 연속성을 유지하기 위한 것이다(노, 2004). 한국산업기술보호협회와 지식경제부가 공동으로 2008년 8월에 1176개 기업 및 기관을 상대로 정보보안 수준을 조사하였다. 조사결과를 보면 하드웨어 측면에 해당하는 물리적, 기술적 보안은 상대적으로 만족도와 효과가 높은 반면에 소프트웨어 측면에 해당하는 관리적, 인적 보안은 상대적으로 낮은 수준으로 나타났고, 특히 인적보안이 가장 낮은 수준으로 조사되었다.

정보기술의 발달과 네트워크 기술의 확산으로 모든 조직에서는 정보 유출가능성이 높은 실정이다. 특히 항만은 국가의 생존과 직결되는 사회간접자본이며, 현대의 항만에서는 물류의 흐름을 정보의 흐름으로 대변할 수 있다. 최근에 와서 항만에서는 인터넷, RFID, GPS, WiFi, Smart 기술 등 새로운 정보기술을 다른 산업에 비하여 신속하게 도입하고 있으며, 이러한 정보기술의 도입으로 항만 효율화를 달성하고 있다. 또한 항만분야는 화주, 선사 및 포워더, 운송사, 컨테이너터미널 운영사, 관세청, 국토해양부 등 다양한 주체가 공급망을 구축하고 있고, 공급망 내에서 정보의 흐름이 단절될 경우 공급망 전체의 업무가 마비될 수 있는 상황에 놓여 있다. 국내에서도 항만분야의 정보보안을 위한 노력이 진행되고 있다. 한국수산개발원 보고서(2009)에 따르면 항만분야에서도 정보통신 및 사이버보안의 중요성이 강조되고 있다. 테러가 시설에 대한 테러에서 국가전산망에 대한 테러로 지능화, 고도화됨에 따라 정보통신 및 사이버공간에 대한 보안 요구가 급증하였으며, 각종 정보보안 시스템 개발로 인해 정보통신 및 사이버보안시장 규모는 2009년에서 2019년 사이 연평균 7% 수준으로 성장할 것으로 전망되고 있다. 특히 사이버보안시장의 경우 2009년 115억 달러 규모에서 2019년 170억 달러 규모로 연평균 4% 수준으로 증가할 것으로 전망된다.

이렇듯 항만분야에서 정보보안의 중요성이 증대하고 있고, 그와 관련된 몇몇 연구들이 진행되어 왔다. 항만분야에서 정보보안과 관련된 선행연구를 살펴보면 조직 차원에서의 정보보호 수준 평가나 항만보안관리 분석모델에 정보관련 평가항목을 포함하는 연구가 진행되어 왔다(이, 2009; 정, 2012). 국내의 정보보안 수준들 중에서 특히 관리적, 인적 보안 수준이 낮은 수준이고, 이(2009)의 연구에서도 관리적, 물리적, 시스템 보안 수준들 중 관리적 보안 수준이 상대적으로 물리적 보안 수준보다 낮은 결과를 보이고 있다. 따라서 본 연구에서는 항만기업 종사자 개인의 정보보안인식 수준이나 지각된 정보보안위험의 정도를 파악할 연구의 필요성을 인식하였다.

본 연구의 목적은 항만기업 종사자들의 정보보안인식 정도와 지각된 정보보안위험 정도에 영향을 미치는 요인들이 어떤 것들이 있는 지를 실증 분석하는 것이다. 특히, 지각된 정보보안위험에 영향을 미치는 요인을 위험분석방법론을 토대로 분석하고자 한다.

2. 정보보안 관련 연구 및 정보보안을 위한 위험분석방법론

2.1 조직의 정보보안 및 정보보안인식 관련 연구

정보보안이란 정보의 입력, 처리, 저장, 출력, 전송 등의 모든 단계에 걸쳐서 정보시스템을 보호하는 것을 말한다(박 등, 2011). 또한 정보보안은 내·외적인 위협들로부터 조직의 손실을 최소화하고 이익을 극대화하는 것을 의미한다(Finne, 1998). 과거 조직에서는 대부분 시스템을 통해 중앙집권적으로 조직을 통제 할 수 있었기에 기술적인 측면을 중심으로 정보보안에 대해 접근을 시도하였지만, 현재 조직에서는 효과적인 보안대책이라고 할 수 없다(Dhillon and Backhouse, 2000).

Dhillon and Backhouse(2000)은 시스템을 사용하는 주체이자 책임자가 인간이기 때문에 정보시스템 보안 관련하여 사회적, 조직적 이슈가 중요하다고 지적하였다. 또한 Straub and Nance(1990)는 조직구성원의 정보보안 행동을 정보보안교육, 보안 관련 보상이나 처벌을 통해 적절하게 통제하게 된다면 내부 조직구성원에 의한 보안사고 뿐만 아니라, 조직 외부 사항에 연관된 보안사고까지 어느 정도 예방적인 차원에서 관리가 가능하다고 보고 있다.

Broderick(2001)은 조직의 자원을 적절하게 관리하기 위하여 위험 분석 작업이 수행되어야 하며 운영방법, 업무의 변경이 있을 때 효과적인 위험관리가 수행되어야 한다고 하였다. 또한 새로운 위협 요인이나 취약성이 있을 때 정기적으로 위험분석이 수행되고 유지되어야 한다고 보았다.

기업의 정보보안인식이란 조직 내 직무를 수행함에 있어 개인이 정보보안 중요성을 알고 있는 정도를 말한다. 지식정보화 시대에서 기업 정보화는 기업이 경쟁력을 가지기 위한 지원도구이자 기업의 생존도구로 인식되고 있다. 하지만 높은 정보화 수준과는 달리 정보에 대한 무단 유출, 파괴, 변조 등이 나타나고 있으며, 또한 불법적인 사용자에 의한 정보시스템의 파괴, 개인 신상 비밀의 누설 및 유출, 불건전 정보의 유통 등과 같은 피해도 증가하고 있다. 따라서 기업에서는 정보보안 문제를 단순히 정보시스템이나 정보기술에 국한된 것이 아닌 조직 전반에 걸쳐 다루어야 될 문제로 인식해야 한다. 뿐만 아니라 정보를 이용하고 관리하는 사람들의 윤리의식 문제를 심각하게 고려해야 할 필요성을 인식해야 할 것이다.

Nosworthy(2000)는 조직에서의 정보보안정책은 정보보안을 위한 관리수단이며 정책을 실행시키고 운영하는데 중요한 방향으로 수립되어야 조직구성원의 정보보안인식을 제고시킬 수 있다고 하였다. 정보보안정책은 조직의 중요한 자산 피해를 예방할 수 있다고 주장하였다. 또한 정보보안정책 사항에 대한 조직구성원들의 실패의 원인이 정보보안에 대한 인식 부족이며, 자

원 할당 부족 및 교육과 훈련의 부족에 기인한다고 주장하고 있다. 따라서 정보보안 실패를 방지하고, 정보보안인식 제고를 위해 조직의 정책적인 측면에서의 표준화된 정보보안교육과 보안훈련이 필요하다고 하였으며 이에 대한 프로그램 라이프사이클 모형을 제시하였다.

Rezgui and Marks(2008)는 정보보안인식에 있어서 탐색적 연구를 수행하여 정보보안교육의 중요성을 주장하였다. 학습된 환경에서 정보시스템 보안인식이 촉진되며, 정보보안인식 향상에 대한 기대를 할 수 있다고 주장하였다. 정보시스템 보안정책을 통하여 사용자에게 높은 교육이 시행되고 기관에서 제공하는 훈련이 잘 시행되었을 때 기본적으로 정보시스템 보안 관리를 위한 지침들을 더 잘 준수하게 되며, 보안관련 이슈들은 정보보안인식 캠페인을 통해 관심도를 높이게 된다. 또한 정보시스템 보안 인식의 평가함에 있어 보상과 처벌이라는 측면을 도입하여 조직의 정보보안에 대한 책임감을 높이고, 정보의 가치를 보다 더 소중히 여기는 정보보안인식을 높일 수 있을 것으로 주장하고 있다.

McCoy and Fowler(2004)는 정보시스템 사용과 관련한 보안이슈를 통해 정보보안인식에 경각심을 일깨워 줄 수 있음을 제시하였다. 이에 대한 방안으로 온라인에서는 뉴스레터, 이메일, 포털사이트, 인터넷 방송국, 동영상 광고 등을 통해서 보안광고를 하며, 오프라인에서는 포스터를 통한 보안광고를 내세우기도 한다. 또한 조직이나 단체에서는 정보보안인식을 증진시키기 위해 포스터를 이용한 보안공익광고를 제시하기도 하며, 일간지, 주간지, 잡지 등 서적을 통한 보안광고를 하면서 전반적인 보안의 중요성을 인식시켜주며, 정보시스템사용자들의 관심도 향상에 기여한다.

Spurling(1995)은 정보보안의도를 회사의 내부 정보를 보호하기 위한 행동의지로 정의하였으며, 조직의 중요정보 유출에 대하여 정보보안의도를 가지고 있을 때 정보보안인식에 보다 긍정적인 영향을 미친다고 하였다.

따라서 기업 구성원의 정보보안인식의 증진을 위해서는 정보보안교육과, 정보보안관심도, 그리고 정보보안의도 등이 중요한 변수임을 알 수 있다.

2.2 정보보안을 위한 위험분석방법론

정보시스템의 보안위험 관리를 위한 위험분석방법론은 정보와 정보기술 서비스로부터 적절한 수준의 기밀성, 무결성, 가용성을 달성하고 유지하기 위한 하나의 과정이다(김, 2000; 이, 2004). 즉, 위험분석방법론은 정보자산에 대한 식별 및 평가, 위협 및 취약성 평가로 구성되는 위험분석 과정을 통해 위험을 측정하여 분석하는 절차와 방법을 의미한다(Rainer et al., 1999). 위험분석은 정보자산의 가치와 위협 및 취약성 평가의 결과를 토대로 위험분석을 수행하는 과정으로 구성된다.

1) 정보보안위험

위험의 정의는 다양하며, 정보보호 업계에서 가장 많이 사용되는 표현은 국제표준기구(International Standards Organization : ISO)에서 만든 정보보호 관리를 위한 지침이다. 이 지침에 따르면 위험은 “어떤 특정한 위협이 자산 또는 자산 그룹의 취약성을 이용하여 자산에 손상 또는 손실을 야기할 수 있는 가능성”으로 정의되며, 위험의 영향 또는 상대적 심각성은 손상 또는 손실의 사업적 가치와 위협의 추정빈도 수에 따라 결정된다(Rainer et al, 1991; CSE, 1996). 따라서 위험은 다음과 같은 구성요소를 가지고 있다. 첫째, 물리적 자산과 정보자산을 포함하는 자산 또는 프로세스의 취약점과 자산 및 프로세스에 대한 위협이다. 둘째, 위협과 취약성으로 인한 자산에 대한 영향이다. 마지막으로 위협의 발생 가능성으로 발생빈도와 가능성의 조합이다. 정보시스템 운영 관리에서 위험분석 과정은 보호 대상이 정보시스템 자산의 가치와 상호 의존도를 파악하고 자산에 손해를 미칠 수 있는 위협들의 유형을 파악하여, 각 위협의 강도와 빈도를 측정하는 위협 분석 수행과 동시에 자산이 보유하고 있는 취약성을 평가하는 과정을 포함하고 있다. 이러한 검토분석 과정을 거쳐서 조직이 보유한 정보시스템 자산 가치와 위협 및 취약성 평가의 결과를 토대로 위험을 측정, 평가하는 과정으로 구성된다. 본 연구에서는 정보보안위험을 어떤 특정한 위협이 정보자산 또는 정보자산 그룹의 취약성을 이용하여 자산에 손상 또는 손실을 야기할 수 있는 가능성으로 보고자 한다.

2) 정보자산

조직에서 자산의 관리는 조직 목표 달성을 위한 관리의 핵심적 요소이며, 모든 관리 계층의 주요한 임무이다(NIST, 2001). 조직의 자산은 물리적 자산, 정보자산, 소프트웨어 자산, 상품자산, 인적자산, 무형자산 등으로 구분될 수 있다(문·박, 2002). 물리적 자산은 정보시스템 하드웨어, 통신장치, 사무집기, 건물 등이며, 정보자산은 데이터베이스 자료, 전산 파일, 서류문서 등이다. 소프트웨어 자산은 응용프로그램, 패키지 소프트웨어 등이며, 인적자산은 관리 및 기술 전문 인력 등이다. 무형자산은 사회적 이미지, 상표권, 영업권, 특허권, 의장권, 전문지식 등으로 분류할 수 있다. 이러한 모든 자산은 위험으로부터 보호되어야 할 충분한 유·무형의 가치가 있다. 조직의 자산이 명확히 정의되고 가치가 평가되지 않는다면 해당 자산을 보호하기 위한 방법과 계획의 수립이나 구현이 불가능하다(CMU/SEI, 1999). 위험분석의 첫 번째 단계는 보호되어야 할 자산을 식별하고 분석하는 것이다. 자산을 식별하기 위해서는 많은 노력이 요구되므로 시간 및 비용의 제약조건을 고려해 구체적 분석 수준을 결정해야 하며 이러한 분석 수준은 정보시스템의 보안 목적에 기초하여 결정되어야 한다. 본 연구 대상인 항만기업에서 운영 관리되는 정보보호 자산을 평가하기 위해 고려되어야 할 중요한 점은 자산 간의 상호 의존성이다. 자산은 취약성에 의해 위협에 노출되며, 자산의 가치가 증가함에 따라 그 위협도 증가하게 된다.

3) 위협

위협분석이란 자산에 해를 입힐 수 있는 가능한 모든 위협들을 규정하고 적절한 방법으로 분류하여 각각의 성질을 파악하는 것이며, 위협평가는 이러한 위협들의 발생 확률 또는 빈도와 자산에 해를 입히는 정도를 평가하는 것을 말한다(NIST, 2001). 위협은 자산이 가진 고유의 취약성을 이용하여 자산을 노출시켜 자산이 소유한 가치에 직/간접적인 피해를 줄 수 있으며, 위협이 증가함에 따라 위험이 증가하게 된다. 위협은 그 원천이 자연적인가 또는 인위적인가로 구별될 수 있으며, 인위적 위협은 다시 고의적 또는 우발적 위협으로 구분될 수 있다. 또한 위협은 조직의 일부부분에만 손상을 끼치는 경우, 특정 위치 정보시스템에 한정되어 영향을 주는 경우, 그리고 조직 내에 존재하여 흔히 간과되기 쉬운 경우 등이 있다(Loch et al., 1992). 위협이 초래하는 손상이 일시적이거나 또는 자산의 파괴와 같이 영속적일 수 있으며 직접적인 이익 손실부터 간접적인 신뢰의 손실까지 다양하다. 어떤 위협들은 그들이 초래하는 손상의 정보가 일관성이 있을 수 있으며 이런 경우에는 공통적 접근 방법이 사용될 수 있는 반면, 손상의 정보가 일관적이지 못할 경우에는 개방적 접근방법이 더욱 적절하다. 위협을 고려할 때는 위협의 발생 빈도를 고려해야 하고 일반적으로 발생빈도는 조직이 경험한 과거 자료나 일반적 통계치를 이용하여 구하며, 이와 같은 자료가 부재 시에는 주관적 인식에 의해 위협의 빈도를 추정할 수 있다.

4) 취약성

취약성은 자산이 고유하게 가지고 있는 약점으로서 위협에 의해서 이용된다(NIST, 2001). 위협은 자산이 가지고 있는 취약성을 이용하여 자산에 피해를 줄 수 있기 때문에 취약성이 증가하게 되면 위협 또한 증가하게 된다. 즉 위협을 감소시킬 수 있는 보안대책이 부족할 경우에 취약성이 증가하게 되며 취약성, 위협, 보안대책은 밀접하게 관련되어 있다(CSE, 1996). 또한 취약성은 위협에 의해 공격을 당해 원하지 않는 사고를 초래하여 정보시스템에 손상을 줄 수 있으며, 단순히 위협이 자산에 영향을 줄 수 있는 조건을 제공 할 뿐 취약성 자체로 인해 손실이 발생하는 것은 아니다(엄, 2003). 취약성 분석은 위협에 이용될 수 있는 취약성을 찾아내고, 심각성을 분석하는 것이다. 특정 정보시스템에 있어 모든 취약성이 위협으로부터의 공격대상이 되는 것은 아니며 취약성에 대응하는 위협이 있어야만 자산에 손실을 초래하게 된다.

3. 연구모형 및 가설설정

3.1 연구모형

본 연구에서는 지금까지 논의된 사항들을 토대로 항만기업 종사자의 정보보안인식 정도와 지각된 보안위험의 정도에 영향을 미치는 요인을 살펴보고자 Fig. 1과 같이 연구모형을 설계하였다.

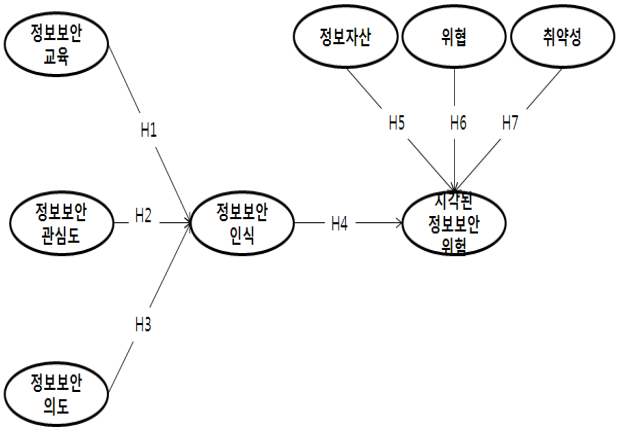


Fig. 1 Research model

본 연구에서 실증분석 대상기업을 항만기업으로 선정한 근거를 제시하면 다음과 같다. 항만기업은 새로운 정보기술을 타 산업에 비해 신속하게 적용하여 효율성을 높이고 있다. 따라서 그에 따른 정보유출가능성도 타 산업보다 높고, 특히, 항만을 중심으로 구축되어 있는 공급망에서 정보보안과 관련된 문제가 발생할 경우에 공급망 전체가 손해를 입을 가능성이 매우 높다. 또한 해상보안사고의 위협대상에 선박, 화물, 선원에 대한 정보관리 및 관련사항 유지관리, 해상운송 파트너들과의 보안관련 데이터에 대한 호환성 관리 등이 포함되어 있어서 항만에서의 정보보안에 대한 중요성을 보여주고 있다(정, 2012). 항만에서 정보보호수준을 평가한 결과를 보면 물리적 보안수준에 비하여 관리적, 시스템 보안수준은 상대적으로 낮은 수준임이 확인되었다(이, 2009). 이러한 점을 반영하여 본 연구에서는 항만기업 종사자의 관리적, 인적 보안수준을 파악할 수 있는 정보보안인식 정도와 지각된 정보보안위험 정도에 영향을 미치는 요인들을 실증분석을 통해 확인하고자 한다.

본 연구의 목적을 달성하기 위하여 첫째, 정보보안인식의 선행요인으로 정보보안교육, 정보보안관심도, 보안의식 등의 요인으로 구성하였다. 둘째, 위험분석방법론을 토대로 정보자산, 위협, 취약성 요인들과 지각된 정보보안위험과의 관계를 규명하고자 하였다. 마지막으로 항만기업 종사자의 정보보안인식과 지각된 정보보안위험과의 관계를 규명하고자 한다.

3.2. 연구가설

1) 정보보안인식과 선행요인 간의 관계

정보보안교육은 정보보안에 관련된 특강, 교육, 훈련, 세미나 등을 모두 포함하여 조직 구성원이 얼마만큼 유익하다고 생각하고 있는지에 대한 평가로 효과를 측정할 수 있다. White (1998)는 정보보안교육의 세부내용으로 사이버윤리에 대한 이해, 기초 암호학 이해, 네트워크, 통신기술, 물리적 보안, 정보보호 대책 보안, 취약점 분석 보안, 감사 사업지속성 관리, 애플리케이션 보안, 정보보호관련 법률, 직업윤리사이버법률 등의 교육을 들었다. 이(2003)는 최근 컴퓨터 및 정보통신기술 등의 급속한 발전과 국가 정책에 따른 세계최고수준의 IT인프라구축에

따라 인터넷이용률 및 인터넷에 의한 범죄 등이 급증하고 있는 것을 나타내면서 정보보안교육의 필요성을 언급하였다. Ronald et al.(2007)은 정보보안교육수준이 보안행동의식에 긍정적 영향을 미치는지에 대한 연구를 수행하였다. 연구 대상은 대학생 1학년부터 4학년까지로 선정하였으며, 정보보안교육의 중요성의 관점에서 논의되었는데 분석결과 대학 신입생은 고학년에 비해 컴퓨터보안과 범죄에 대해서 대체적으로 보안인지수준이 낮은 것으로 나타났다. Straub and Nance(1990)와 Hawkins et al.(2000)은 정보보안교육 수준이 보안 행동인식에 미치는 중요한 영향요인임을 증명하였다. 개인이 속한 조직이나 단체에서는 정기적으로 정보보안교육을 실시를 한다. 이러한 정보보안교육은 기업의 내부자료, 중요정보 등 개인의 자산뿐만 아니라 조직의 자원을 보호하기 위해서 중요한 요소이다. 따라서 항만기업에서도 구성원들의 정보보안교육이 정보보안인식에 긍정적인 영향을 미친다는 가설을 도출하였다.

H1: 정보보안교육은 정보보안인식에 정(+)의 영향을 미친다.

Carrie et al.(2004)은 정보보안관심도가 보안행동인식에 긍정적인 영향을 미치는 요인으로 작용한다고 보았으며, 정보보안관심도를 광고적인 차원에서 세부적으로 살펴보았다. 조직이나 단체에서는 보안에 대한 경각심을 고취시키기 위해서는 온라인 혹은 오프라인 채널을 통하여 보안 광고활동을 촉진하고 있다. 광고는 사람들의 내재된 인지적 요소 변화에 영향을 주는 중요한 수단으로 작용한다고 할 수 있다. 연구 분석결과 윤리적인 판단에 대한 호소를 원할 때 온라인, 오프라인, 모바일, TV 광고 등에서 제공하는 공익성을 띄는 보안광고를 통해 정보보안관심도를 축적해 나갈 수 있으며, 자신이 정보보안관심도를 가지고 있는 사람이라고 판단되는 것은 그러한 광고에 의한 반응이 적극적이면 관심도가 높다고 볼 수 있다. 즉, 정보보안관심도를 지닌 상태에서의 정보보안인식은 긍정적인 영향을 가져다 줄 수 있다. 따라서 항만기업 종사자들의 정보보안관심도가 정보보안인식에 긍정적인 영향을 미친다는 가설을 도출하였다.

H2: 정보보안관심도는 정보보안인식에 정(+)의 영향을 미친다.

Hawkins et al.(2000)은 정보보안의도를 네트워크 환경에서 인터넷을 통해 유출되는 위험에서 보호하려는 의지로 보았으며 네트워크 환경이 발달함에 따라 정보유출이 될 수 있는 확률이 많아지기에 이에 따른 명확한 정보보안인식의 중요성을 언급하였다. Petrova and Sinclair(2003)은 정보보안의도를 전자상거래 과정에서의 보안위협적인 요소들과 보안대응을 위한 방안들, 보안기술을 적용하여 정보를 보호하려는 행동의지로 분석하였다. 전자상거래 이용자에게 보안에 대한 행동의지가 전자상거래 활성화를 위한 정보보안인식에 긍정적인 영향을 주는 것으로 나타났다. 따라서 항만기업 종사자들의 정보보안의도는 정보보안인식에 긍정적인 영향을 미친다는 가설을 도출하였다.

H3: 정보보안의도는 정보보안인식에 정(+)의 영향을 미친다.

2) 정보보안인식과 지각된 정보보안위험 간의 관계

정보보안인식은 조직 내 직무를 수행함에 있어 개인이 정보보안 중요성을 알고 있는 정도를 말한다. 조직원들의 정보보안교육, 보안의 관심도, 보안의식이 높게 측정될수록 정보보안위험에 대해 심각하게 받아들이는 현상을 확인할 수 있다. 임(2006)은 정보보안인식은 조직구성원이 직무를 수행하는데 있어서 정보보안의 함축된 상태를 잘 알 수 있도록 하는 프로세스라고 정의하였다. 정보보안의 중요성을 인식하고, 보안사고 발생 시 대응방안에 대해 구체적으로 알고 있으면, 보안을 위한 체계 등을 제시할 수 있으며, 정보보안위험에 적극적인 관심도를 가질 수 있다. Choi et al.(2008)은 정보보안인식은 조직 전체의 정보보안성과의 핵심지표이며 보안 위협으로부터 정보시스템의 성공적인 보호에 가장 결정적인 요소로 등장하였으며 조직의 정보보안 활동에 있어서 사전에 먼저 고려되어야 함을 강조하였다. NIST(2002)에서는 인식의 목적은 단지 정보보호에 대한 주의를 집중시키는 것이며 인식 표현은 개인이 IT 정보보호에 대한 관심을 가지고 이에 대한 반응을 보이도록 하는 것이라고 하였다. 즉, 반응도가 높을수록 정보보안과 연관한 정보보안위험이 높게 측정될 수 있기에 정보보안인식은 정보보안위험에 긍정적인 영향을 미친다. 따라서 항만기업 종사자들의 정보보안인식이 높을수록 정보보안위험에 긍정적인 영향을 미친다는 가설을 도출하였다.

H4: 정보보안인식은 지각된 정보보안위험에 정(+)의 영향을 미친다.

3) 지각된 정보보안위험과 선행요인 간의 관계

정보자산 분석 시 고려해야 할 중요한 점은 자산 간의 상호의존성을 고려하여 수행해야 하며, 자산은 취약성에 의해 위협에 노출되며, 자산의 가치가 증가함에 따라 그 위험도 증가하게 된다(한국정보통신기술협회, 2003). 자산은 조직의 정보시스템과 관련된 것으로 정보자산에 포함되며, 개인정보, 조직의 내부문서, 업무관련 문서 등을 포함하고 있다(ISO/IEC, 2005). Rainer, et al.(1991)는 위험분석에서의 자산 중 업무 관련 정보가 무엇보다도 중요함을 언급하였으며, Haller(2002)는 기업 내부에서의 사원들의 신상정보를 포함한 개인정보의 중요성에 대해 제시하였다. 이는 자산의 중요도가 높을수록 정보유출 정보보안위험성도 높다고 볼 수 있다. 자산의 가치가 중요할수록 개인정보의 중요성을 포함하는 경우가 많으며 이러한 정보자산이 유출되었을 때의 피해도 심각함을 알 수 있다. 항만분야에서 정보자산은 매우 중요한 자산이다. 항만과 관련된 공급망에서는 EDI기술을 통하여 정보공유가 이루어지고 있는데, 정보자산에 손실이 발생할 경우 하나의 기업이 아니라 공급망 전체에서 손실을 입게 된다. 따라서 항만기업 종사자들이 항만기업의 정보자산에 대한 중요성을 높게 인식할수록 정보보안위험을 지각하는 정도가 긍정적인 영향을 미친다는 가설이 도출되었다.

H5: 정보자산은 지각된 정보보안위험에 정(+)의 영향을 미친다.

위협은 자산이 가진 고유의 취약성을 이용하여 자산을 노출시켜 자산이 소유한 가치에 직/간접적인 피해를 줄 수 있으며 위협이 증가함에 따라 위험이 증가하게 된다(BSI, 2005). 홍·이(2000)는 기업의 경쟁업체의 스파이침입으로 인한 위협을 제시하면서 기업데이터의 중요성을 언급하였다. 위협분석이란 자산에 해를 입힐 수 있는 가능한 모든 위협들을 규정하고 적절한 방법으로 분류하여 각각의 성질을 파악하는 것이며, 위협평가는 이러한 위협들의 발생 확률 또는 빈도와 자산에 해를 입히는 정도를 평가하는 것을 말한다. 항만분야는 새로운 항만이 구축되면서 국내 뿐만 아니라 세계적으로 경쟁이 치열해 지고 있으며 그에 따라 산업스파이로부터 위협을 받을 가능성도 높아지고 있다. 따라서 본 연구에서는 위협을 항만기업의 정보자산의 보안에 침해를 가져다 줄 수 있는 원인이나 행위의 정도로 보고 항만기업의 정보자산에 대한 위협이 높을수록 지각된 정보보안위험도 높게 나타날 것이라는 가설을 도출하였다.

H6: 위협은 지각된 정보보안위험에 정(+)의 영향을 미친다.

취약성은 정보 환경과 기존의 보안대책을 고려하여 현존하는 위협의 공격대상이 될 수 있는 자산의 약점을 알아내고, 이런 취약점이 정보나 정보자산에 어떤 위협을 야기 시킬 수 있는 지를 파악하고 분석한다(NIST, 2001). 즉, 특정 정보시스템 또는 정보 데이터 자산의 고유 약점을 이용하여 위협에 얼마나 쉽게 손상 될 수 있는지 측정하는 것이 취약성을 분석하는 목적이다. 특정 정보시스템에 있어 모든 취약성이 위협으로부터의 공격대상이 되는 것은 아니며 취약성에 대응하는 위협이 있어야만 자산에 손실을 초래하게 된다. 항만기업의 정보자산은 항만공급망에서 정보공유를 필요로 하기 때문에 네트워크를 통한 이동이 빈번하게 일어나고 있는데 이와 같은 상황으로 인해 정보자산은 보안에 취약성을 내포하고 있다. 본 연구에서의 취약성은위협에 의해 항만기업의 정보자산 보안에 부정적인 영향을 줄 수 있는 정보자산의 속성 혹은 상태로 평가하고자 한다. 따라서 취약성이 높을수록 지각된 정보보안위험 정도에 긍정적인 영향을 미친다는 가설을 도출하였다.

H7: 취약성은 지각된 정보보안위험에 정(+)의 영향을 미친다.

3.3 연구변수의 조작적 정의 및 설문항목

본 연구의 연구모형과 가설설정에 사용된 변수들의 측정도구들에 대한 조작적 정의는 Table 1에서 보는 바와 같다. 조작적 정의는 측정에 앞서 정의된 변수의 개념적 정의를 보다 구체적인 형태로 표현한 것으로 실증검증에 전제되는 관찰가능성, 즉 측정가능성과 직결된 정의이다. 항만조직의 정보보안위험에 영향을 미치는 요인에 대한 연구를 중심으로 검정하기 위한 연구 개념들을 다음과 같이 조작적으로 정의하였으며, 모든 측정항목은 리커트(Likert) 7점 척도로 설문항목을 구성하였다.

Table 1 Item of research conception

연구 요인	조작적 정의	설문항목	참고문헌
정보 보안 교육	조직의 정보보안 교육(특강, 훈련, 세미나 등)에 대한 개인의 평가 사항의 정도	-정보보안교육 내용 -정보보안교육 방식 -정보보안교육 활동성 -정보보안교육 적용성	White(1998) Ronald et al.(2007) Hawkins et al.(2000)
정보 보안 관심도	정보보안에 관한 경각심을 고취시킬 수 있는 정보보안관심도의 정도	-정보보안 TV광고 관심도 -정보보안 최신뉴스 관심도 -정보보안 웹사이트 광고 관심도 -정보보안 포스터 관심도	Carrie et al.(2004)
정보 보안 의도	조직의 내부의 정보보호를 위해 개인이 중요시 하는 정보보안 방안의 중요성을 의식하여 보호하려는 행동의지 정도	-패스워드 변경 -공인 인증서 보관 -바이러스 검사 -데이터 백업	Hawkins et al.(2000) Petrova and Sinclair (2003)
정보 보안 인식	조직구성원의 직무수행에 있어 정보보안의 중요성을 알고 있는 정도	-신상정보 보안 중요성 -패스워드 보안 중요성 -프로그램 보안 중요성 -데이터 보안 중요성	임(2006) Choi et al.(2008)
지각된 정보 보안 위험	어떤 특정한 위협이 정보자산 또는 정보자산 그룹의 취약성을 이용하여 자산에 손상 또는 손실을 야기할 수 있는 가능성에 대하여 조직구성원이 지각하고 있는 정도	-중요정보의 공개 가능성 -금전적 손해 가능성 -데이터 유출 가능성 -신상정보 공개 가능성	NIST(2001) Pounder (2003)
정보 자산	조직의 정보유출에 대해 보호되어야 할 정보자산으로 조직의 데이터 파일, 업무관련 정보, 패스워드 관련 업무 등의 중요성 정도	-데이터파일 중요성 -프로그램 정보의 중요성 -업무관련 정보의 중요성 -사원정보의 중요성	ISO/IEC (2000) Rainer(1991) Haller(2002)
위협	조직의 정보자산의 보안에 침해를 가져다 줄 수 있는 원인이나 행위의 정도	-산업스파이의 정보 도난 가능성 -산업스파이의 정보 침입 가능성 -산업스파이의 기업데이터 접근 가능성 -경쟁업체의 정보 접근 가능성	홍·이(2000) Loch et al.(1992)
취약성	위협에 의해 조직의 정보자산 보안에 부정적 영향을 끼칠 수 있는 조직정보자산의 잠재적인 약점	-보안관리 취약성 -인원관리의 취약성 -사고대책관리의 취약성 -경영절차관리의 취약성	NIST(2001)

4. 분석결과

4.1 표본선정 및 분석기법

본 연구에서는 항만기업 종사자들의 정보보안인식과 지각된 정보보안위험에 영향을 미치는 요인을 평가하기 항만기업 종사자들을 표본집단으로 선정하여 설문을 수행하였다. 연구모형의 분석을 위해 전체 300부의 설문을 배포하여 268부를 회수하였으며, 결측치가 있거나 불성실하게 응답한 20부의 설문지를 제외한 총 248부를 최종분석에 활용하였다. 수집된 데이터는 응답

자의 인구통계적 특성분석을 위해 SPSS Windows 15.0이 사용되었으며, 연구모형의 적합성을 검증하기 위해 적용된 구조방정식 모델의 평가를 위해 AMOS 7.0으로 분석하였다.

본 연구의 표본특성은 아래의 Table 2와 같다. Table 2에서 응답자의 표본특성을 살펴보면 남자가 215명(86.7%), 여자가 33명(13.3%)으로 나타났으며, 연령대는 30~40세 미만이 107명(43.1%), 40~50세 미만이 96명(38.7%)을 차지하였다. 또한, 응답자가 재직 중인 조직유형으로 터미널 및 운영사가 109명(44%), 물류정보기술 관련기업이 82명(33.1%), 종합물류기업 37명(14.9%)을 차지하고 있었다. 직급으로는 실무자가 198명(79.8%)으로 가장 많은 비중을 차지하고 있었으며, 근무 년 수는 10년 이상이 129명(52%)로 절반이상 차지하는 것으로 나타났다. 그리고 조직의 규모를 나타내는 종업원 수는 1000명 이하 119명(48%), 300명 이하 83명(33.5%)으로 나타났다. 따라서 항만기업 종사자들의 정보보안인식과 지각된 정보보안위험에 영향을 미치는 요인들을 실증분석을 할 수 있는 표본의 특성을 갖추었다고 볼 수 있다.

Table 2 Characteristics of the sample

구분	항목	빈도수	비율(%)
성별	여자	33	13.3
	남자	215	86.7
연령	20~30세 미만	34	13.7
	30~40세 미만	107	43.1
	40~50세 미만	96	38.7
	50세 이상	11	4.4
조직유형	터미널 및 운영사	109	44
	종합물류기업	37	14.9
	물류정보기술관련기업	82	33.1
	기타	20	8.1
직급	실무자	198	79.8
	단위부서 책임자급	44	17.7
	임원급	6	2.4
근무년수	1년 미만	25	10.1
	1년 이상~3년 미만	28	11.3
	3년이상 ~7년 미만	36	14.5
	7년 이상~10년 미만	30	12.1
	10년 이상	129	52
종업원수	100명 이하	44	17.7
	300명 이하	83	33.5
	1000명 이하	119	48
	1000명 이상	2	8

4.2 측정모형의 신뢰성과 집중타당성

본 연구에서는 확인적 요인분석을 통해 측정 하부모형의 신뢰성을 평가하기 위한 합성개념 신뢰도와 평균분산추출, Cronbach-α값을 검정하였으며, 그 결과는 다음의 Table 3과 같다. 먼저, 각 구성개념들에 대하여 지정된 예측변수가 그들 구성개념을 충분히 설명하고 있는가를 확인하는데 필요한 추정치는 합성개념 신뢰도와 평균분산추출 값(AVE)이다. 먼저 합성개념 신뢰도의 경우에 모든 구성개념이 권장수준인 0.7이상을 상회하는 것으로 나타나 전반적으로 양호한 수준으로 평가되었다. 그 중에서 취약성이 0.97로 가장 높았으며, 다음으로 위협이 0.96, 정보보안인식과 위협이 0.93, 정보보안관심도가 0.92, 정보보안의도가 0.91, 자산이 0.90으로 나타나 모두 합성개념 신뢰도가 상당히 높게 분석되었다. 그리고 구성개념에 의해서 설명되는 분산의 양을 나타내는 평균분산추출 값(AVE)이 0.5를 상회하는 것으로 나타나 신뢰성을 확보할 수 있었다. 집중타당성의 분석결과 측정모델의 각 항목의 추정치가 0.5이상이며, 그 추정치의 t-값이 2.0 이상으로 나타나 각 측정항목의 집중타당성이 충분한 것으로 판단된다. 또한 Cronbach-α값 권장기준 0.7이상의 수용기준에 부합되고 있어 측정항목의 구성개념에 대한 신뢰성이 확보되었음을 알 수 있다

Table 3 Measurement model analysis

요인	항목		집중타당성					
		비표준화 추정치	표준화 추정치	t-값	측정 오차	합성 개념 신뢰도	AVE	Cronbach-α
정보보안 교육 (SE)	SE1	0.79	0.76	13.30	0.43	0.89	0.68	0.82
	SE2	1.00	0.86	-	0.26			
	SE3	0.90	0.82	14.64	0.33			
	SE4	0.85	0.86	12.42	0.27			
정보보안 관심도 (SC)	SC1	0.91	0.83	17.52	0.31	0.92	0.73	0.85
	SC2	0.91	0.84	17.90	0.29			
	SC3	1.00	0.89	-	0.20			
	SC4	0.92	0.85	18.06	0.28			
정보보안 의도 (SI)	SI1	1.00	0.73	-	0.46	0.91	0.72	0.79
	SI2	0.91	0.75	11.33	0.4			
	SI3	0.98	0.87	13.15	0.24			
	SI4	0.95	0.81	12.30	0.35			
정보보안 인식 (SA)	SA1	0.90	0.85	16.55	0.38	0.93	0.77	0.89
	SA2	1.00	0.99	-	0.03			
	SA3	0.68	0.81	19.52	0.35			
	SA4	0.82	0.90	26.88	0.19			
지각된 정보보안 위험 (RSK)	RSK1	0.84	0.86	20.75	0.26	0.93	0.78	0.88
	RSK2	0.85	0.80	18.01	0.36			
	RSK3	0.98	0.95	27.19	0.10			
	RSK4	1.00	0.92	-	0.15			
정보자산 (AS)	AS1	1.00	0.90	-	0.19	0.90	0.69	0.82
	AS2	0.99	0.89	20.68	0.20			
	AS3	0.93	0.88	20.00	0.23			
	AS4	0.66	0.63	11.28	0.61			
위협 (TH)	TH1	1.00	0.95	-	0.09	0.96	0.86	0.93
	TH2	0.99	0.98	39.43	0.04			
	TH3	0.94	0.93	30.84	0.13			
	TH4	0.87	0.85	21.98	0.28			
취약성 (V)	V1	0.97	0.93	30.26	0.14	0.97	0.88	0.94
	V2	0.99	0.93	29.91	0.14			
	V3	1.00	0.96	-	0.09			
	V4	0.98	0.94	32.51	0.11			

4.3 측정모형의 판별타당성

판별타당성은 각 구성개념들의 평균분산추출 값의 제곱근이 다른 구성개념들 간의 상관계수보다 크면 판별성이 있다고 본다.

Table 4 Measurement model to determine the feasibility

변수	추출된 평균분산의 제곱근 값							
	1	2	3	4	5	6	7	8
1. 정보보안교육	(0.82)							
2. 정보보안관심도	0.58	(0.85)						
3. 정보보안의도	0.52	0.57	(0.85)					
4. 정보보안인식	0.33	0.26	0.55	(0.88)				
5. 지각된 정보보안위험	0.03	0.12	0.09	0.16	(0.88)			
6. 정보자산	0.35	0.33	0.46	0.73	0.23	(0.83)		
7. 위협	0.01	0.05	0.11	0.10	0.64	0.21	(0.93)	
8. 취약성	0.07	0.12	0.04	0.11	0.51	0.28	0.63	(0.94)

( ): 각 변수의 AVE 제곱근

Table 4에서 보는 바와 같이 본 연구의 평균분산추출 값의 제곱근은 각 연구 개념의 상관관계의 수치보다 크게 나타나 판별타당성이 충분하다고 본다.

4.4 모형의 적합도 평가

본 연구모형에 대한 적합도 지수는 다음의 Table 5와 같다. 우선 측정모형의 절대부합지수를 살펴보면 χ^2(p)는 743.71(0.00)이며, χ^2을 자유도로 나눈 비율이 1.74로 권장수준(≤3.00)에 부합하였다. 구조모형의 절대부합지수도 χ^2(p)는 1021.83(0.00)이며, χ^2을 자유도로 나눈 비율이 2.27로 권장수준(≤3.00)에 부합하였다.

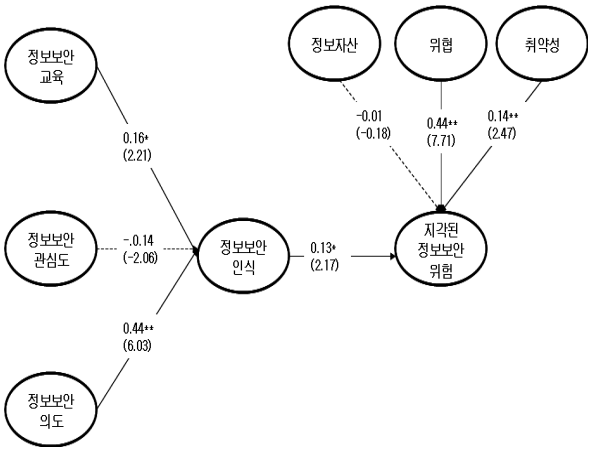
Table 5 Goodness of fit index

구분	적합도지수	수용기준	측정모형 분석결과	구조모형 분석결과
절대부합지수	χ^2/df	≤3.00	1.74	2.27
	χ^2 자유도(df) p-value	≥0.05	743.71 428 0.00	1021.83 450 0.00
	기초부합지수(GFI)	≥0.90	0.84	0.80
	근사원소평균자승잔차(RMSEA)	≤0.08	0.06	0.07
증분부합지수	수정부합지수(AGFI)	≥0.80	0.81	0.77
	표준부합지수(NFI)	≥0.90	0.91	0.88
	관계부합지수(RFI)	1.0근사	0.90	0.86
	증분부합지수(IFI)	1.0근사	0.96	0.93
	비교부합지수(CFI)	≥0.90	0.96	0.93
간명부합지수	간명기초부합지수(PGFI)	≥0.60	0.68	0.69
	간명표준부합지수(PNFI)	≥0.60	0.79	0.80

GFI는 측정모형이 0.84, 구조모형이 0.80으로 권장수준인 0.90보다 약간 낮게 분석되었지만 AGFI가 0.80에 근접하고 있으며, RMSEA는 측정모형이 0.06과 구조모형이 0.07로 나타나 수용기준(≤0.08)을 충족하는 것으로 평가된다. 다음으로 증분적합지수를 살펴보면 IFI가 측정모형이 0.96, 구조모형이 0.93으로 나타났으며 CFI가 각각 측정모형이 0.96, 구조모형이 0.93으로 나타났다. 마지막으로 간명부합지수 PGFI는 측정모형 0.68과 구조모형 0.69로 분석되었으며, PNFI가 0.79, 0.80으로 수용기준을 상회하는 것으로 나타나 대체적으로 측정모형의 적합도와 구조모형 적합도 지수가 수용기준을 충족하는 것으로 나타났다.

4.5 구조모형의 가설검정 결과분석

구조모형의 가설검정 결과에 따르면 각 경로의 추정치와 t-값은 아래의 Fig. 2와 같이 나타났으며, 정보보안관심도와 정보보안인식과의 관계를 나타내는 경로와 정보자산과 지각된 정보보안위험과의 관계를 나타내는 경로를 제외한 다른 모든 경로는 통계적으로 유의한 것으로 확인되었다.



주) 괄호 안은 t-값, *: p<0.05, **: p<0.01에서 유의

Fig. 2 Result of research model

구조모형의 결과에 따라 가설검정을 한 결과는 Table 6에서 보는 바와 같다.

Table 6 Results of hypothesis testing

연구가설	경로계수	t-값	검정결과
[H1] 정보보안교육은 정보보안인식에 정(+)의 영향을 미친다.	0.16	2.12*	채택
[H2] 정보보안관심도는 정보보안인식에 정(+)의 영향을 미친다.	-0.14	-2.06	기각
[H3] 정보보안의도는 정보보안인식에 정(+)의 영향을 미친다.	0.44	6.03**	채택
[H4] 정보보안인식은 지각된 정보보안위험에 정(+)의 영향을 미친다.	0.13	2.17*	채택
[H5] 정보자산은 지각된 정보보안위험에 정(+)의 영향을 미친다.	-0.01	-0.18	기각
[H6] 위협은 지각된 정보보안위험에 정(+)의 영향을 미친다.	0.44	7.71**	채택
[H7] 취약성은 지각된 정보보안위험에 정(+)의 영향을 미친다.	0.14	2.47**	채택

*: p<0.05, **: p<0.01

가설검정결과를 요약하면 다음과 같다.

첫째, 정보보안교육이 정보보안인식에 미치는 영향을 평가하기 위해 설정한 연구가설1(H1)은 경로계수가 0.16으로 나타났으며, t-값이 2.12로 유의수준 $p<0.05$에서 통계적으로 유의한 것으로 나타나 가설을 채택한다.

둘째, 정보보안관심도가 정보보안인식에 영향을 미친다는 연구가설2(H2)의 경우 경로계수가 -0.14,이며, t-값이 -2.06으로 통계적으로 유의하지 않은 것으로 나타나 가설이 기각되었다.

셋째, 정보보안의도가 지각된 정보보안위험에 영향을 미친다는 연구가설3(H3)은 경로계수가 0.44이며, t-값이 6.03으로 유의수준 $p<0.01$에서 통계적으로 유의한 것으로 나타나 채택되었다.

넷째, 정보보안인식이 지각된 정보보안위험에 정(+)의 영향을 미친다는 연구가설4(H4)는 경로계수가 0.13, t-값이 2.17로 나타나 유의수준 $p<0.05$에서 채택되었다.

다섯째, 정보자산과 정보보안위험 간의 관계에서는 경로계수가 -0.01, t-값이 -0.18로 통계적으로 유의하지 않게 나타나 가설이 기각되었다

여섯째, 위협이 지각된 정보보안위험에 영향을 미친다는 연구가설6(H6)은 경로계수가 0.44, t-값이 7.71이고 취약성이 지각된 정보보안위험에 영향을 미친다는 연구가설7(H7)은 경로계수가 0.14, t-값이 2.47로 나타났다. 따라서 두 가설 모두 유의수준 $p<0.01$에서 채택되었다.

5. 결 론

항만산업은 전체적인 물류관리를 효율적으로 수행하기 위하여 필요한 물류정보를 생산하기 위하여 물류산업 전반에 걸쳐서 정보시스템을 구축하여 운행하고 있다. 물류정보란 물류주체 및 거점별로 산재되어 있는 물류데이터를 첨단 기술을 활용하여 연계, 수집, 제공함으로써 물류공급망상에서 단절되어있는 정보의 연속적 흐름을 지원하고 유비쿼터스 환경에 적합한 물류시스템 구현의 기반을 마련하는 데 사용되는 정보이다(김 등, 2009). 따라서 항만기업에서도 체계적인 정보보안관리가 절실히 필요한 상황이다.

본 연구에서는 항만기업 종사자의 정보보안인식과 지각된 정보보안 위험에 영향을 미치는 요인들을 실증분석을 통하여 확인하였다. 항만기업 종사자의 정보보안인식에 영향을 미치는 요인으로 정보보안교육, 정보보안관심도, 정보보안의도를 선정하였으며, 지각된 정보보안위험의 선행요인으로는 위험분석방법론을 기반으로 정보자산, 위협, 취약성 등을 선정하였다.

본 연구의 결과를 요약하면 다음과 같다.

첫째, 항만기업 종사자들의 정보보안인식 정도에 영향을 미치는 요인으로 정보보안교육과 정보보안의도로 나타났다. 반면, 정보보안관심도는 정보보안인식 정도에 영향을 미치지 않는 것으로 나타났다. 정보보안관심도가 정보보안인식에 통계적으로 유의한 결과를 보이지 않고 있는 결과는 다음과 같이 해석될 수 있다. 정보보안관련 TV광고, 최신뉴스, 웹사이트 광고, 포스터 광고 등 본 연구에서 선정한 측정변수들이 보안의 경각심을 일깨워주기 위한 방안으로 주변에서 쉽게 볼 수는 있지만 정작 항만기업 개개인의 정보보안인식에는 큰 도움이 되지 않고 있음을 보여준다. 따라서 항만기업에서 항만기업 종사자들이 정보보안에 대한 관심을 가지고 정보보안인식을 높이기 위해서는 또 다른 정보보안관심도를 높일 수 있는 대안이 필요하다는 것을 알 수 있다.

둘째, 항만기업 종사자들의 지각된 정보보안위험의 정도에 영향을 미치는 요인으로 위협과 취약성이 확인되었다. 반면에 정보자산은 항만기업 종사자들의 지각된 정보보안위험의 정도에 영향을 미치지 않는 것으로 나타났다. 이와 같은 결과는 항만기업 종사자들이 정보자산의 범주를 조직이라는 틀에서 평가하고 있기 때문으로 해석할 수 있다. 즉 아직도 국내 항만기업 종사자들이 조직의 정보자산에 대한 중요성을 크게 인식하지 못하고 있으며, 조직의 정보자산이 유출되었을 때 처하게 되는 조직의 위급상황이나 손해에 대한 인식정도가 낮다는 것을 의미한다. 따라서 항만조직에서도 구성원들의 정보자산에 대한 중요성과 정보보안위험에 대한 지각이 제대로 이루어질 수 있는 정책이나 대안마련이 필요할 것이다.

셋째, 항만기업 종사자들의 정보보안인식은 지각된 정보보안위험에 긍정적인 영향을 미치는 것으로 나타났다. 항만기업 종사자들은 정보보안의 중요성을 알고 있는 정도가 높을수록 정보자산의 취약성을 이용하여 자산에 손상 또는 손실을 야기할 수 있는 가능성에 대하여 높이 지각하고 있음을 알 수 있다.

본 연구는 다음과 같이 학문적 및 실무적 시사점을 갖고 있다.

첫째, 지금까지 항만분야에서 정보보안과 관련된 연구가 미미한 상황에서 항만기업 종사자들을 대상으로 정보보안 연구를 수행하였다는 점이다. 특히 조직에서 물리적, 기술적 보안보다 상대적으로 만족도가 낮은 인적보안 측면을 다룬 점이 학문적 시사점을 제공한다.

둘째, 기존의 항만의 정보보안과 관련된 연구가 항만관련 조직의 정보보호 수준 평가에 초점을 맞추고 있는 상황인데, 본 연구에서는 항만기업 종사자 개개인의 정보보안인식 정도와 지각된 정보보안위험을 다루고 있다는 점이다.

셋째, 실무적으로는 항만기업 종사자들의 정보보안인식과 지각된 정보보안위험의 정도에 영향을 미치는 요인을 제시함으로써 항만기업의 정보보안과 관련된 정책이나 의사결정에 도움을 줄 수 있을 것으로 예상한다. 항만기업에서 불시에 정보유출이나 정보보안과 관련된 다양한 위험이 도사리고 있는 상황에서 조직의 정보보호를 위하여 조직구성원 차원의 관심을 높여나가는 것이 필요하다는 인식을 높일 수 있는 기반을 제공하고 있다.

본 연구의 한계점과 향후 연구과제는 다음과 같다. 첫째, 항만기업의 종사자들을 대상으로 정보보안인식과 지각된 정보보안위험성을 측정하였기 때문에 전 산업에 걸쳐 일반화하는 데는 한계가 있다. 둘째, 정보보안인식에 영향을 미치는 요인들을 보다 광범위한 부류로 분류하여 정보보안인식을 측정할 필요성

이 있다. 예를 들면, 보안관련 교육을 수행하기 이전의 시점과 이후의 시점에서의 조직구성원들의 정보보안인식의 차이도 존재할 것이라는 관점에서 다각도의 차원에서 각 요인을 평가하는 연구수행이 필요하리라 생각된다. 마지막으로 항만기업 종사자들의 특성을 반영한 변수의 도출이 필요하다고 판단된다.

후 기

본 논문은 한국해양대학교의 2010학년도 해외파견 연구교수 지원에 의하여 수행된 연구입니다.

참 고 문 헌

[1] 김수엽, 최종희, 김찬호(2009), 항만물류보안산업의 발전방안 연구, 한국해양수산개발원

[2] 김정덕(2000), ISO 정보기술 보안관리지침 표준화동향, 한국정보보호진흥원

[3] 노순동(2004), “기업체의 효율적인 보안관리 모델”, 산업보안논총 창간호, pp. 79-101.

[4] 문용은, 박유진(2002), “IS 아웃소싱의 위험과 아웃소싱의 정도에 관한 연구”, 정보시스템 연구 11권 1호, pp. 1-28.

[5] 박준경, 김범수, 조성우(2011), “기업 정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인”, 경영학연구 40권 4호, pp. 955-985.

[6] 엄정호(2003), “정보시스템의 체계적인 위험관리를 위한 실용적인 위험감소 방법론에 관한 연구”, 정보처리학회논문지 10권 C호, pp. 125-132.

[7] 이문구(2004), “정보시스템 보안관리를 위한 위험분석 방법론”, 전자공학회논문지 41권 6호, pp. 13-22.

[8] 이민섭(2003) “정규학교에서의 정보보호 교육 강화 방안”, 정보보호학회지 13권 6호, pp. 67-78.

[9] 이재원, 류형근, 안정흠(2010), “국내물류기업의 물류보안 인식에 관한 연구”, 한국항해항만학회지 34권 1호, pp. 45-50.

[10] 이홍걸(2009), “주요 컨테이너 터미널의 정보보호 수준 평가에 관한 연구”, 한국항해항만학회지 33권 10호, pp. 735-742.

[11] 임채호(2006) “효과적인 정보보호인식제고방안”, 정보보호학회지 16권 2호, pp. 30-36.

[12] 정우리(2012), “해상보안관리 분석모델 개발에 관한 연구”, 한국항해항만학회지 36권 1호, pp. 9-14.

[13] 정보통신부(2010), 국가정보보호백서

[14] 홍일유, 이종삼(2000), “국내기업의 정보시스템 보안위협 인식에 관한 연구”, 경영학회지 27권 2-1호, pp. 157-185.

[15] Broderick, J.S.(2001), “Information Security Management - When Should it be Managed?”, Information Security Technical Report, Vol.6, No.3, pp. 12-18.

[16] BSI(2005), Code of Practices for Information Security Management. London: British Standards Institution.

[17] Choi, N., Kim, D and Whitmore, A.(2008), “Knowing is Doing”, Information Management & Computer Security, Vol.16, No.5, pp. 484-501.

[18] CMU/SEI(1999), Operationally Critical Threat, Asset, Vulnerability Evaluation(OCTAVE) Framework, Ver. 1.0, CMU/SEI-99-TR-017. Carnegie Mellon University/ Software Engineering Institute, June.

[19] CSE(1996), Guide to Security Risk Management for IT Systems, Communications Security Establishment, Government of Canada.

[20] Dhillon, G. and Backhouse, J.(2000), “Information System Security Management in the New Millennium”, Communications of the ACM, Vol.43, No.7, pp. 125-128.

[21] Finne, T.(1998), “A Conceptual Framework for Information Security Management”, Computers & Security, Vol.17, No.4, pp. 303-307.

[22] Haller, S. C(2002), “PRIVACY: WHAT Every Manager Should Know”, The Information Management Journal, Vol.36, No.3, pp. 33-44.

[23] Hawkins, S., Yen, D.C. and Chou, D.C.(2000), “Awareness and Challenges of Internet Security”, Information Management & Computer Security, Vol. 8, No.3, pp. 131-143.

[24] ISO/IEC(2005), Guideline for the Management of IT Security(GMITS), International Organization for Standardization/International Electrotechnical Commission.

[25] Loch, K.D., Carr, H.H. and Warkentin, M.E.(1992), “Threats to Information Systems: Today's Reality, Yesterday's Understanding”, MIS Quarterly, Vol.16, No.2, pp. 173-186.

[26] McCoy, C and Fowler, R.T.(2004), “You are the Key to Security :Establishing a Successful Security Awareness Program”, ACM SIGUCCS Conference, No.32, pp .346-349.

[27] NIST(2001), Security Self-Assessment Guide for Information Technology Systems. Special Publication 800-26.

[28] NIST(2002), Risk Management Guide for Information Technology Systems. Special Publication 800-30.

[29] Nosworthy, J. D.(2000), “Implementing Information Security in the 21st Century-Do You Have the Balancing Factors?”, Computers & Security, Vol.19, No.4, pp. 337-347.

[30] Petrova, K., Sinclair, R.(2003), “Expanding the Understanding: Transactions and Security Awareness for Business Students”, New Zealand Journal of

Applied Computing and Information Technology, Vol.7, No.1, pp. 82-88.

[31] Pounder, C.(2003), “Security with Unfortunate Side Effects”, Computers & Security, Vol.22, No.2, pp. 115-118.

[32] Rainer, R., Snyder, C. and Carr, H.(1991), “Risk Analysis for Information Technology”, Journal of Management Information System, Vol.8, No.1, pp. 129-147.

[33] Rezgui, Y. and Marks, A.(2008), “Information Security Awareness in Higher Education: an Exploratory Study”, Computers & Security, Vol.27, No.7, pp. 241-253.

[34] Ronald, C., Curtis, C. and Aaron, J.(2007), “Phishing for User Security Awareness”, Computer & Security, Vol.26, pp. 73-80.

[35] Spurling, P.(1995), “Promoting Security Awareness and Commitment”, Information Management & Computer Security, Vol.3, No.2, pp. 20-26.

[36] Straub, D. and Nance, W.(1990), “Discovering and Disciplining Computer Abuse in Organizations: A Field Study”, MIS Quarterly, Vol.14, No.1, pp. 45-60.

[37] White, S.(1998), “Open Problems in Computer Virus Research”, Virus Bulletin Conference, Oct 22.

원고접수일 : 2012년 2월 20일
심사완료일 : 2012년 4월 23일
원고채택일 : 2012년 4월 25일