Journal of Korea Port Economic Association, Vol.28, No.1, 2012, 1-23.

해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인

강다연* · 장명희**

Factors Influencing on the Compliance of Information Security Policy of Workers of Shipping and Port Organization

Dayeon Kang · Myunghee Chang

Abstract : Advances in information technology has brought many benefits to businesses, but at the same time, businesses are facing serious problems caused by its use such as information leakage. In order to cope with problems, companies have established information security policies, demanding workers of a company to be compliant with the policies. This study proposes a research model that includes information security awareness, information security attitude, self-efficacy, standard belief and social influences as factors that affect the compliance of information security policy among the workers of shipping and port organization. The results of this study showed that there was a positive relationship not only between the information security awareness and the information security attitude, but also between the information security attitude and the information security policy among the workers of shipping and port organization. It was also found that there was a positive relationship between the self-efficacy and the compliance of information security policy, and between the social influence and the compliance of information security policy. However, there was no meaningful relationship between the standard belief and the compliance of information security policy. This study examined to what extent the workers of shipping and port organization that have a high possibility of the information leakage were compliant with the information security policy. The findings will contribute to organizations of shipping and port who attempt to establish strategies related to information security.

Key Words : Shipping and Port Organization, Information Security Awareness, Information Security Attitude, Compliance of Information Security Policy

▷ 논문접수: 2012.01.30 ▷ 심사완료: 2012.03.26 ▷ 게재확정: 2012.03.28

* 한국해양대학교 해운경영학부 강사, mswcrash@hanmail.net, 051)410-4384, 대표집필
** 한국해양대학교 해운경영학부 부교수, cmhee2004@hhu.ac.kr, 051)410-4384, 교신저자

Ⅰ. 서 론

정보기술의 발전은 기업에게 많은 이익을 가져다주었지만, 정보유출이라는 심각한 문제를 야기하고 있다. 보안업체인 트렌드마이크로는 소니, RSA 등 지능형지속가능위협(APT : Advanced Persistent Threat) 공격의 사고사례가 대거 발생했던 2011년을 '데이터 유출의 해'로 규정하고 있다(디지털데일리, 2010. 1. 26). 지능형지속가능위협(이하 APT) 공격기법은 내부 시스템에 침투할 수 있도록 사전에 치밀하게 내부 시스템과 관리자 등을 파악한 뒤 이에 알맞은 악성코드를 제작해 감염시킨다. APT 공격에 사용되는 악성코드는 감염여부도 인식하지 못하고 PC에서 최장 670일을 잠복했던 피해도 나타난 바 있다. 특히 최근 발생하고 있는 대부분의 해킹 피해가 APT 공격이지만 기존 보안 기술로만으로는 막기가 쉽지 않아 더욱 문제가 되고 있다. 3500만명의 정보가 유출된 네이트 · 싸이월드의 해킹사례도 APT의 공격으로 인한 것이라는 것이 전문가들의 분석이다. 국가정보원 산업기밀보호센터에서 집계한 자료에 따르면, 최근 5년간 총 가치 50조원에 육박하는 189건의 국내 기업 핵심 기밀 유출사건이 있었던 것으로 조사되었다. 기업 내 정보유출 유형 중 외부로부터의 해킹 공격 등에 의한 정보 유출 외에도 임직원 또는 퇴사자가 업무용 PC에서 기업 내부 자료를 직접 유출하는 사례도 많은 것으로 나타났다. 기존에 기업들은 정보 보안을 위해 파일에 권한을 부여하여 접근을 제한하는 DRM(Digital Rights Management)이나, 모든 애플리케이션과 자료를 서버에서 관리하는 SBC(Server Based Computing)방식을 주로 이용해 왔다. 그러나 최근에는 사용의 편이성과 보안수준을 한 단계 더 높인 형태의 가상 데스크톱이나 파일보안서버 형태의 문서중앙화 솔루션을 도입하는 움직임이 활발해지고 있다. 최근 삼성전자, LG CNS 등은 내부자료 유출을 줄이기 위하여 클라우드 컴퓨팅을 통해 업무용 PC의 본체를 없애고, 모든 파일을 중앙 서버에서 관리하는 '가상 데스크톱' 업무 환경을 도입하고 있다(전자신문, 2011. 9.7).

해운·항만산업은 전체적인 물류 관리를 효율적으로 수행할 수 있도록 물류산업의 각 주체 또는 정부관련 부처들이 개별 또는 통합된 물류 정보시스템 네트워크를 구축하여 운영하고 있다. 이러한 해운·항만산업에서도 정보시스템 리스크 관리가 중요함에도 불구하고 물류정보시스템의 주된 관심분야가 물류비 절감, 정보공유 및 생산성 향상에 주로 초점을 맞추고 있기 때문에 정보시스템과 관련된 다양한 리스크에 대비하지 못하고 있다(장명희, 2009). 해운항만조직에서도 정보보안문제가 대두되고 있으며 이에 대한 노력이 있어 왔다. 부산항만공사의 BDIS(Busan Distripark Information Systems) 시스템은 ASP (Application Service Provider)사업으로 부산항만공사 서버에 모든 정보들이 모이는 구조로 설계되어 있다. 이 시스템은 인터넷을 통해 어디서든 접근 가능한

웹기반시스템으로 개방형 프로토콜로 인한 보안문제가 애로사항이었다(물류신문, 2010. 10). 따라서 부산항만공사는 기능적으로 다양한 방법을 통하여 보안문제를 해결하고자 노력하여 입력 및 수정 권한이 없을 경우 조회밖에 할 수 없도록 원천 차단하고, 사용자 비밀번호 등의 주요항목을 암호화하고 인증 실패횟수를 관리해 접근이 제한되도록 조치하고 있다. 또한 관리측면에서는 서버가 있는 전산실의 경우 자체적으로 연 1회 이상 정보보안감사를 진행하고 있다.

기업들의 정보유출에 대한 기업자체의 방어노력이 구체화되고 있으며, 학계에서도 많은 연구가 이루어지고 있는 실정이다. 정보유출 및 정보보안에 대한 연구는 보안 위협에 대한 개인행동이나 보안 기술을 사용하는 조직 구성원을 대상으로 한 연구가 주를 이루고 있다(Goodhue and Straub, 1991; Straub and Welke, 1998). 최근에 와서는 기업의 정보와 시스템을 보호하기 위해서 관리적 측면이 강조되고 있다. 즉, 효과적인 보안정책을 세워서 이를 조직구성원들이 실행할 수 있도록 동기부여를 하는 것이 중요하다는 연구에 관심을 가지기 시작했다(Amitava and McCrohan, 2001).

그러나 해운항만조직에서 정보보안 문제는 중요하게 다루어야 할 문제임에도 불구하고 정보보안과 관련된 연구는 아주 미미한 실정이다. 특히 해운항만조직에서도 기술적인 측면의 정보보안 뿐만 아니라 효과적인 보안정책을 강화할 필요성이 있음에도 불구하고 관련 연구는 찾아보기가 힘들다.

따라서 본 연구의 목적은 다음과 같다. 첫째, 정보보안정책 준수와 관련된 이론과 선행연구를 통하여 해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인들을 도출하여 연구모형을 구축한다. 둘째, 해운항만조직 구성원들에 대하여 설문조사를 통하여 정보보안정책 준수에 영향을 미치는 요인이 어떠한 것들이 있는지를 확인하고자 한다. 마지막으로 분석결과를 바탕으로 해운항만조직 구성원들의 정보보안정책 준수 정도를 파악하여 해운항만조직의 정보보안정책 수립 시 참고할 수 있는 프레임워크를 제공하고자 한다.

Ⅱ. 정보보안정책 준수 평가항목 및 선행연구

1. 조직의 정보보안정책의 특징

정보보안정책(Information Security Policy)이란 기업이 보유하고 있는 비밀 및 정보를 다양한 위험으로부터 보호하고, 불법적인 정보유출을 사전에 예방하여 기업의 가치 및 정보자산의 손실을 최소화하기 위한 기업의 정책을 규정한 것이다(Halibozek & Kovacich, 2005; 노순동, 2004). Russell and Gangemi(1991)에 따르면 보안정책이란 조

직의 중요 정보를 어떻게 관리하고 보호하며, 배포하는가에 관한 일련의 규칙과 실무지침을 규정해 놓은 것으로 정보시스템 활용에 있어 사용자와 조직구성원들에게 보안관련 기준을 제시해 놓은 것이다. 또한, 조직의 정보보안정책이란 정보보안 접근성에 대해 인증된 사용자에게 권한을 허용하는 권한부여와 이에 따른 권한은 접근통제라는 비인가된 접근으로 부터 방지하는 기능을 제공한다.

기업의 정보보안정책은 구성 원칙에 따라 3단계의 체계로 구성하는 것이 바람직하다. 그 체계는 규정, 규칙, 기준의 순서로 구성된다. 규정의 경우 최상위의 정책을 의미하며, 모든 임직원들에게 공표될 포괄적인 원칙을 정의한 것으로 다음과 같은 사항이 포함되어야 한다. 보안규칙에서는 규정에서 정한 원칙을 시행하기 위해 필요한 관리 영역별로 절차 등을 기술하여야 하며, 프로세스 관점에서 효율적인 통제와 관리가 이루어질 수 있도록 각종 보호대책 수립 및 관리시스템 등의 도입을 고려하여야 한다(노순동, 2004). 특히, 조직 내의 정보보안은 조직 활동과 관련된 자산, 인적자원의 정보를 중요도에 따라 각종 위협과 취약성으로부터 보호하는 활동이라 할 수 있다(노민선과 이삼열, 2010). 정보보안정책이라는 것이 매우 포괄적인 의미를 가지고 있으며, 조직구성원이 속한 범주 안에서의 기업 내 정보보안을 위한 각 정책 가이드라인이 상이하기에 일반적으로 보안정책에는 조직구성원이 준수하고 있는 이행정도를 정보보안인식의 차원에서 바라보는 관점이 필요하다.

기업의 정보보안 중요도에 따른 피해를 최소화 시키는 방안들 중의 하나가 조직의 정보보안정책을 조직구성원들이 준수하고 있는지 확인하는 것이다. 기업이 자산 및 자원을 적절히 보호하기 위해 필요한 관리적·운영적·기술적 통제 및 보호 장치에 관한 최소한의 보안을 위해 지식과 책임을 가지는 것이 우선적으로 해결해 나가야할 과제이며, 이를 수반하는 것이 바로 조직의 정보보안정책이라고 할 수 있다. 즉, 조직의 정보보안정책을 잘 준수하면 기업의 보안목표와 비전에 부합하는 역할과 책임에 대한 이해를 할 수 있으며, 근본적인 보안정책, 절차, 및 적절한 이행을 통해 조직 내의 중요한 정보자산, 정보위협, 그리고 정보취약성과 관련된 위험요소에 대한 사전 대응력을 높일 수 있다.

2. 정보보안태도

Ajzen and Fishbein(1997)은 개인의 태도를 주어진 문제에 대해 긍정적 혹은 부정적인 방식으로 응답하는 감정으로 정의하고, 특정 정보를 통해 좋거나 나쁜 감정을 학습하게 되어 행동의도보다 선행된다고 하였다. 합리적 행위이론(The Theory of Reasoned Action; TRA)과 계획된 행동이론(Theory of Planned Behavior; TPB)모형에

서도 태도는 행동에 대한 믿음과 결과로부터 형성되는 것으로 설명하고 있다(Davis, 1989). 즉, 어떤 대상에 대해 일관성 있게 호의적 또는 비호의적으로 반응하는 것이 개인의 느낌이나 감정을 통해 표현되는 심리학적 경향이라고 정의한다(Eagly and Chaiken, 1993). Rundmo and Sjoberg(1998)는 조직 내에서 개인 사용자들이 정보보호에 대한 위험을 의식하여 행동하는 것이 정보보안태도라고 보았으며, 위험행위에 대한 보안방안으로의 태도가 형성된다고 하였다. 보안에 대한 태도는 위험 행위와 관련되어 살펴볼 수 있다. 본 연구에서는 태도를 정보보안관점에서 바라보았으며, 정보보안을 위하여 해운항만조직의 구성원들이 가지는 호의적인 정보보안태도의 정도로 평가하고자 한다.

3. 자기효능감, 규범신념, 사회적 영향

자기효능감은 주어진 과제나 행동을 성공적으로 수행할 수 있다는 개인의 성공가능성에 대한 신념으로, 행동의 선택과 수행, 그리고 그 지속성에 영향을 미친다. 이러한 자기효능감 이론에 기초하여 많은 연구들이 개인의 자기효능감 지각이 그 개인의 직무성과와 직무만족에 긍정적인 영향을 미친다는 것을 보여주고 있다. Bandura(1977)는 이와 같은 관점에서 인간행동의 변화가 결국 행위자 자신이 그 행위를 능히 해낼 수 있다는 기대 때문에 일어난다는 점을 강조하여 성취상황에서 개인이 가질 수 있는 기대로서 효능기대감과 결과기대감을 제시하고 그 개념적 차이는 다음과 같이 제시하였다. 자기효능감이 결과기대보다 동기와 더 밀접히 관련되어 있다고 한다. 왜냐하면 개인의 어떤 행동과정이 어떤 결과에 이르게 할 것인지 믿을 수 있더라도 만일 자신이 그런 행동을 성공적으로 수행할 수 없다고 확신하게 되면 결과기대는 행동동기에 영향을 주지 않기 때문이다. 어떤 상황에 직면하였을 경우 사람들은 자신이 그 상황에 대처할 수 있다는 능력이 있다고 여길 때에는 자신 있게 대처행동을 수행하게 된다. 따라서 개인은 특정행동이 어떤 결과를 가져올 것이라고 믿을 수 있지만 자신이 그 행동을 할 수 있을 것인가에 대해서는 의문을 가지기 때문에 효능기대와 결과기대는 구별이 된다. 본 연구에서의 자기효능감은 해운항만조직의 정보보안을 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 해운항만조직 구성원 개인의 기대감 정도로 평가하고자 한다.

기업이나 정부조직은 정보시스템에 대한 의존도가 지속적으로 증가하고 있지만 정보자산에 대한 위협에 많은 투자를 하지 못하고 있는 상황이다. 체계적인 정보보호를 위해서 조직은 정보보호정책의 확립이 필수사항이다. 조직의 적절한 정보보호정책수립 및 실행은 조직의 내재적인 가치 및 경쟁력을 증가시키는 역할을 할 수 있도록 규범적 신

념을 형성하도록 한다(Siponen, 2000). 조직구성원의 보안정책과 관련된 규범에 대한 신념도가 높을수록 보안정책을 잘 준수하기 위한 행동이 나타난다고 할 수 있다. 본 연구에서는 규범신념을 조직의 정보보안 강화를 위해 보안정책 규범을 긍정적으로 받아들이는 믿음의 정도를 평가하여 해운항만조직 구성원들의 규범신념을 확인하고자 한다.

인간의 행동과 심리적 특성을 연구 하는데 있어, 개인의 사회적인 행동과 개인에게 미치는 사회영향은 매우 중요할 뿐만 아니라, 인간의 개인적 행동 연구와 더불어 심리학의 핵심 연구 대상이라고 할 수 있다(Rice, 1990). 사회적 영향이란 어떤 변화를 일으키는 데 영향을 미치는 힘으로, 개인 혹은 집단의 태도나 행동을 바꾸는 데 작용하는 사회적 힘을 포함한다. 영향이란 과업 수행에 대한 전략적, 관리적, 운영적 결과에 대하여 개인이 영향을 미칠 수 있는 정보를 뜻한다(Thomas and Velthouse, 1990). 즉, 조직적 결과에 대한 통제의 정도로 바라볼 수 있으며, 사회적 영향은 조직에서의 전략적 의사결정에도 참여할 수 있는 영역으로 본다. 따라서 본 연구에서는 사회적 영향을 해운항만조직 구성원들이 정보보안정책 준수를 함에 있어 사회적으로 미치는 영향 정도로 평가하고자 한다.

4. 정보보안정책 준수와 관련 연구

정보보호정책은 조직 구성원의 행동방향을 제시할 수 있으며, 정보자산에 대한 위협과 공격에 대한 대응을 하기 위해 조직에 속한 구성원의 인식 제고에 기반이 된다. 따라서 조직의 적절한 정보보호정책 수립 및 실행은 조직의 내재적인 가치 및 경쟁력을 증가시키는 역할을 한다(Siponen, 2000). 보안 강화를 위해서 잘 정의되고 검증된 보안정책은 조직의 구성원들로부터 안전성과 신뢰성을 확보할 수 있으며, 이러한 보안정책을 수립하기 위해서는 고려해야할 요소는 조직의 구성원의 이해와 시행에 혼선을 초래하지 않는 보안정책이어야 하며 조직의 목표, 기술능력, 보안요구의 변화 등에 따라 융통성을 가질 수 있어야 하기 때문에 경직된 보안정책이 되어서는 안 된다.

Bulgurcu et al.(2010)은 조직의 보안정책 동의의도에 영향을 미치는 요인에 관한 연구에서 추론기반 신념과 정보보안인식 측면에서 보안정책의 동의의도를 살펴보았다. 우선 정보보안인식을 정보보안정책에 관한 인식과 일반적 인식으로 구분하여 측정하였다. 정보보안인식에 영향을 미치는 요인으로 신념에 관한 산출변수를 본질적 이익, 안전성, 보상, 업무장애, 본질적 비용, 취약성, 제제규정으로 선정하였으며, 신념에 관한 결과의 전체평가를 응낙이익, 응낙비용, 비응낙 비용 요인으로 선정하여 조직구성원들의 태도에 영향을 미치는지를 확인하였다. 마지막으로 정보보안정책의 동의의도에 영향을 미치는 요인으로 태도, 규범신념, 자기효능감으로 선정하여 분석하였다. 실증분석 결과에 따

르면 조직구성원의 정보보안정책 의도에 영향을 미치는 선행요인들 모두가 유의한 결과로 나타났다. 각 요인들의 중요성과 정보보안정책 의도를 가져다 줄 수 있는 노력을 강조하였으며 조직구성원의 정보보안태도, 규범신념, 자기효능감 등 각 특성요인이 최종적인 정보보안정책 준수의도에 긍정적인 영향을 줄 수 있는 요인임을 증명하였다.

Johnston and Warkentin(2010)은 정보보안 행위의도를 개인정보시스템 보안에 관한 지각된 위협에 따라서 구분하였다. 지각된 위협의 정도에 따라 정보시스템 최종사용자의 보안준수제정 방안에 대해서 행동의도에 영향을 미치는 선행요인을 반응효능, 사회적 영향, 자기효능감으로 구분하였으며 통계적으로 유의한 결과로 분석되었다. 사회적 영향에 따라 보안관심도와 관련된 사항을 이해하는 관점이 적극적으로 나타났으며, 자기효능감의 정도가 높을수록 보안행동의도에 긍정적인 영향을 미치는 것으로 나타났다.

Knapp et al.(2006)은 인지된 보안 효과에 영향을 주는 요인으로 최고관리자의 지지, 사용자 훈련, 보안문화, 정책관련성, 정책실행으로 선정하였다. 최고관리자의 지지는 인지된 보안 효과에 긍정적인 영향을 미쳤으며, 최고관리자의 지지는 사용자의 훈련, 보안문화, 정책관련성, 정책실행에 의해 인지된 보안효과를 가져다주는 유의한 결과가 나왔다.

박준경 등(2011)은 기업 정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향요인에 관한 연구에서 기업의 노력에 대한 개인의 인식과 보안에 관련된 개인적 측면이 개인의 정보보호태도에 어떠한 영향을 미치는 지를 연구하였다. 이들의 연구에서 기업의 노력에 대한 개인의 인식을 나타내는 한 가지 변수로 보안정책 유용성 변수가 사용되었다.

본 연구에서는 정보보안정책 준수를 해운항만조직의 정보보안을 위해 규정된 정보보안정책의 준수사항을 받아들이는 해운항만조직 구성원들의 생각의 정도로 평가하고자 한다.

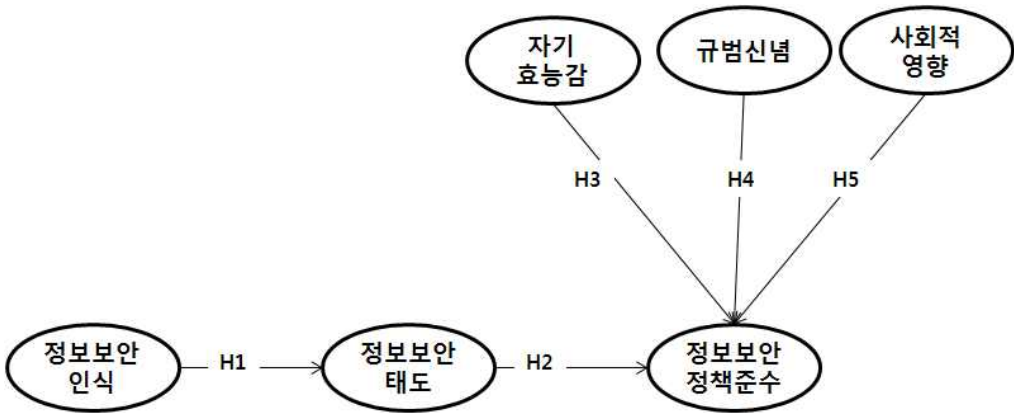
Ⅲ. 연구 설계

1. 연구모형 및 가설설정

본 연구에서는 선행연구에서 논의된 사항들을 토대로 해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인을 살펴보고자 <그림 1>과 같이 연구모형을 설계하였다. 우선 해운항만조직 구성원들의 정보보안인식이 정보보안태도에 긍정적인 영향을 미칠 것이라는 가설과 이에 따른 정보보안태도가 정보보안정책 준수에 긍정적인 영

향을 미칠 것이라는 가설을 설정하였다. 또한 해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 선행요인으로 자기효능감, 규범신념, 사회적 영향 요인으로 구성하였다.

<그림 1> 연구모형



Carrie and Rebecca(2004)는 정보보안인식을 정보보안에 대한 중요성을 의식하여 알고 있는 정도로 보았으며, 정보보안 자산인 개인정보의 중요성뿐만 아니라 조직에서의 데이터의 중요성 인식도 강조하였다. Stanton et al.(2005)은 정보보안인식을 정보시스템 내의 정보유출과 관련하여 위험을 인식하여 행동하는 정도로 보았으며 이는 개인이 가지고 있는 컴퓨터에 관한 기술적 능력이 정보유출을 막는 긍정적 요소로 작용할 수 있는 정보보안태도와 관련 있다고 하였다. 따라서 해운항만조직 구성원들의 정보보안인식은 해운항만조직 구성원들의 정보보안태도에 긍정적인 영향을 미친다는 가설을 도출하였다.

H1: 정보보안인식은 정보보안태도에 정(+)의 영향을 미친다.

특정한 행위와 관련된 행동 의도는 개인이 해당 행위를 수행 할 것인지 혹은 수행하지 않을 것인지에 대한 결정 요인으로써 사용자의 행동지향적인 태도로부터 형성된다(Peace et al., 2003). 즉, 조직구성원들이 정보보안을 위한 여러 활동들에 대한 긍정적인 평가를 하는 것은 조직의 정보시스템을 보호하기 위해서 수립된 조직의 제반 규정과 절차를 잘 준수하기 위한 강력한 의지를 형성할 수 있다. 따라서 해운항만조직 구성원들의 정보보안태도는 해운항만조직 구성원들의 정보보안정책 준수에 긍정적인 영

향을 미칠 것이라는 가설이 도출되었다.

H2: 정보보안태도는 정보보안정책 준수에 정(+)의 영향을 미친다.

자기효능감은 경험을 통한 인지적, 사회적, 언어적 심지어 육체적 능력을 점진적, 복합적으로 획득해 가는 과정에서 형성되며 수준, 강도, 일반성의 3가지 차원에 따라 실제의 행동성취에 중요한 영향을 미치며 각기 그 영향력의 정도는 다르게 나타난다(Bandura, 1977; Gist, 1987). 자기효능감의 수준은 달성할 수 있다고 믿는 과업이 어느 정도 어려운 과업인지를, 자기효능감의 강도는 정말로 달성할 수 있다고 생각하고 확신하는 정도를 그리고 자기효능감의 일반성은 자신의 과업수행 능력에 대한 믿음이 특수한 몇몇 과업의 수행에만 적용될 수 있는지 아니면 보편적으로 일반화 될 수 있는 것인지를 말한다. 본 연구에서는 자기효능감을 해운항만조직의 정보보안을 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 개인의 기대감 정도라고 생각하고 자기효능감이 정보보안정책 준수에 긍정적인 영향을 미칠 것이라는 가설을 도출하였다.

H3: 자기효능감은 정보보안정책 준수에 정(+)의 영향을 미친다.

정보보안강화를 위해서 잘 정의되고 검증된 정보보안정책은 조직의 구성원들로부터 안전성과 신뢰성을 확보할 수 있으며, 이러한 보안정책을 수립하기 위해서 고려해야 할 요소는 조직구성원의 이해와 시행에 혼선을 초래 하지 않는 보안정책 이어야 한다(정보통신부, 2010). 잘 정립된 보안정책은 조직구성원에게 정보보안의 강화를 위한 방안의 지침으로 활용할 수 있으며, 이러한 정보보안 강화를 위한 규범신념을 갖게 한다(Siponen, 2000). 조직 정보보안에 대한 정책관련 규범신념도가 높아지게 되면 보안정책을 잘 준수하기 위한 행동으로 나타난다. 따라서 해운항만조직 구성원들이 가지는 규범신념은 해운항만조직 구성원들의 정보보안정책 준수에 긍정적인 영향을 미친다는 가설을 도출하였다.

H4: 규범신념은 정보보안정책 준수에 정(+)의 영향을 미친다.

Venkatesh et al.(2003)은 정보기술 채택에 있어서 사회적 영향이 중요한 요인으로 작용하고 있음을 검증하였다. 특히 새로운 정보기술에 대한 적응경험이 없거나 잘 알지 못하는 정보기술을 채택할 때는 주변 사람의 영향을 많이 받게 되는 것으로 알려져 있다. 특히, 상호작용성이 강한 정보기술 매체일 경우, 사회적 네트워크에 의한 수용이 강

하게 나타날 가능성을 강조했다. 이는 곧 사회적 영향에 의한 확산이 혁신적 시스템과 서비스를 선택하는 중요한 요인이 될 수 있다는 것을 의미한다. 조직의 정보보안정책 역시 정보시스템과 관련 있는 사항으로 정보보안 관리적인 측면에서 정책의 규정을 준수하는데 사회적인 영향을 크게 받을 것이다. 따라서 사회적 영향은 해운항만조직 구성원들의 정보보안정책 준수에 긍정적인 영향을 미친다는 가설을 도출하였다.

H5: 사회적 영향은 정보보안정책 준수에 정(+)의 영향을 미친다.

2. 연구변수의 조작적 정의 및 항목

연구변수의 조작적 정의는 측정에 앞서 정의된 변수의 개념적 정의를 보다 구체적인 형태로 표현한 것으로 실제검증에 전제되는 관찰가능성, 즉 측정가능성과 직결된 정의이다. 해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인을 검정하기 위해 연구 개념들은 아래의 <표 1>과 같이 조작적으로 정의되었으며, 모든 측정항목은 리커트(Likert) 7점 척도로 설문항목을 구성하였다.

본 연구의 연구변수에 대한 조작적 정의는 조직의 정보보안정책 준수와 관련된 평가항목과 관련된 선행연구들을 기반으로 정의하였다. 기존연구에서 해운항만조직 구성원들을 대상으로 정보보안정책 준수와 관련된 연구가 수행되지 못한 관계로 본 연구에서는 지금까지 연구된 연구변수들 중에서 본연구의 목적을 달성하는데 적합하다고 판단되는 변수들을 선정하고 그에 따른 측정도구들로 설문지를 구성하였다.

정보보안인식에 대한 조작적 정의는 해운항만조직 내에서 직무를 수행함에 있어 조직구성원 개인이 정보보안의 중요성을 알고 있는 정도라고 정의한다. 현대 해운항만물류의 흐름은 정보의 흐름이라 해도 과언이 아니다. RFID, SMART 기술의 도입으로 해운항만조직에서는 물류흐름에 대한 정보관리가 용이해졌다. 그러나 신기술이 가져다주는 이점도 있지만, 개방된 프로토콜의 사용으로 인해 정보유출문제도 심각해지고 있다. 따라서 해운항만조직 구성원들의 정보보안인식 정도를 측정하기 위해서 구성원 개인의 신상정보, 패스워드, 프로그램, 데이터에 대한 보안의 중요성을 설문항목으로 구성하였다.

정보보안태도에 대한 정의는 해운항만조직의 정보보안 방안을 위해 조직구성원들이 가지는 호의적인 정보보안태도의 정도라고 본다. 해운항만조직에서 정보관리와 정보유출로 인한 문제가 발생할 가능성에 대해 구성원들이 가지는 정보보안태도를 측정하기 위하여 컴퓨터 안전성 검증, 보안프로그램 업데이트, 스팸메일 필터링, 주기적 패스워드 변경 정도로 설문항목을 구성하였다. 해운항만조직 구성원들이 매일 물류정보를 다루고

있기 때문에 정보유출에 대한 가능성도 높으며, 따라서 정보보안태도 역시 호의적일 때 해운항만조직의 정보보안도 지켜질 것이다.

<표 1> 연구변수의 조작적 정의 및 항목

연구요인	조작적 정의	설문항목	참고문헌
정보보안인식	해운항만조직 내에서 직무를 수행함에 있어 조직구성원 개인이 정보보안의 중요성을 알고 있는 정도	-신상정보 보안중요성 -패스워드 보안중요성 -프로그램 보안중요성 -데이터 보안중요성	임채호(2006) Choi et al.(2008)
정보보안태도	해운항만조직의 정보보안 방안을 위해 조직구성원들이 가지는 호의적인 정보보안태도의 정도	-컴퓨터 안전성 검증 -보안프로그램 업데이트 -스팸메일 필터링 -주기적 패스워드 변경	Jeffrey(2005)
자기효능감	해운항만조직의 정보보안을 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 조직구성원 개인의 기대감 정도	-보안정책 인지정도 -보안정책 습득정도 -보안정책 적용정도 -보안정책 적응정도	Bandura(1977) Gist(1987)
규범신념	해운항만조직의 정보보안 강화를 위해 조직구성원들이 보안정책 규범을 긍정적으로 받아들이는 믿음의 정도	-보안정책 안전성 -보안정책 신뢰성 -보안정책 우수성 -보안정책 적용성	Siponen(2000)
사회적 영향	해운항만조직 구성원들의 정보보안 정책 규정을 준수하는데 있어서 사회적으로 인지되고 평가된 사항을 반영하는 정도	-사회적 인지도 -사회적 평가 -사회적 유행 -타인의 권유	Venkatesh et al.(2003)
정보보안정책 준수	해운항만조직의 정보보안을 위해 규정된 보안정책의 준수사항을 조직구성원들이 받아들이는 생각의 정도	-보안활동 실제 적용의도 -보안활동 이행의도 -보안활동 조사의도 -보안활동 효과 의도	Halibozek & Kovacich(2005)

정보보안정책 준수의 선행요인으로 자기효능감, 규범신념, 사회적 영향을 선정하였다. 이들 세 요인은 지금까지의 연구들에서 정보보안정책 준수의 선행요인으로 가장 많이 다루어왔고 실증분석을 통해 지지지고 있는 요인으로써 해운항만조직의 구성원들의 정보보안정책 준수의 선행요인으로서도 무리가 없는 것으로 판단하였다.

자기효능감은 해운항만조직의 정보보안을 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 조직구성원 개인의 기대감 정도로 정의하였다. 자기효능감을 측정하기 위하여 정보보안정책의 인지, 습득, 적용, 적응 정도로 설문항목을 구성하였다.

규범신념은 해운항만조직의 정보보안 강화를 위해 조직구성원들이 보안정책 규범을 긍정적으로 받아들이는 믿음의 정도로 정의하였다. 규범신념을 측정하기 위하여 보안정책의 안전성, 신뢰성, 우수성, 적용성 정도로 설문항목을 구성하였다.

사회적 영향은 해운항만조직 구성원들의 정보보안 정책 규정을 준수하는데 있어서 사회적으로 인지되고 평가된 사항을 반영하는 정도로 정의하였다. 사회적 영향을 측정하기 위하여 정보보안정책을 준수하는데 있어 사회적 인지도, 사회적 평가, 사회적 유행, 타인의 권유가 영향을 미치는 정도로 설문항목을 구성하였다.

마지막으로 정보보안정책 준수에 대해서는 해운항만조직의 정보보안을 위해 규정된 보안정책의 준수사항을 조직구성원들이 받아들이는 생각의 정도로 정의하였다. 정보보안정책 준수정도를 측정하기 위하여 보안활동의 실제 적용의도, 이행의도, 조사의도, 보안활동 효과 의도의 정도로 설문항목을 구성하였다. 해운항만조직에서 차지하는 정보의 중요성이 커짐에 따라 정보보안을 위한 정책을 마련하고 그러한 정책을 조직 구성원들이 잘 지켜나갈 때 조직의 내재적인 가치와 경쟁력이 높아질 것이다.

Ⅳ. 실증분석

1. 분석기법 및 표본의 특성

본 연구에서는 해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인을 평가하기 위해 현재 재직 중인 해운항만조직에 속한 구성원들을 표본 집단으로 선정하여 설문을 수행하였다. 연구모형의 분석을 위해 전체 200부의 설문을 배포하여 183부를 회수하였으며, 결측치가 있거나 불성실하게 응답한 5부의 설문지를 제외한 총 178부를 최종분석에 활용하였다. 수집된 데이터는 응답자의 인구통계적 특성분석을 위해 SPSS Windows 15.0이 사용되었으며, 연구모형의 적합성을 검증하기 위해 적용된 구조방정식 모델의 평가를 위해 AMOS 7.0으로 분석하였다.

<표 2>에서 보는 바와 같이 응답자의 표본특성을 살펴보면 남자가 153명(86.4%), 여자가 24명(13.6%)으로 나타났으며, 연령대는 30~40대가 77명(43.5%)으로 가장 높게 나타났으며, 다음으로 40~50대가 68명(38.4%)를 차지하였다. 또한, 응답자가 재직 중인 조직유형으로 터미널 및 운영사가 82명(46.3), 물류정보기술 관련기업이 59명(33.3%), 종합물류기업 23명(13%)을 차지하고 있었다. 직급으로는 실무자가 141명(79.7%)으로 가장 많은 비중을 차지하고 있었으며, 근무 년 수는 10년 이상이 94명(53.1%)로 과반수 이상으로 나타났다. 그리고 조직의 규모를 나타내는 종업원 수 1000명 이하 87명(49.2%), 300명 이하 63명(35.6%)으로 분석되어 해운항만조직 내의 정보보안정책이 규

정되어있는 표본 집단으로 적절하다고 판단하였다.

<표 2> 인구통계학 특성 분석

구분	항목	빈도수	비율(%)
성별	여자	24	13.6
	남자	153	86.4
연령	20~30세 미만	23	13
	30~40세 미만	77	43.5
	40~50세 미만	68	38.4
	50세 이상	9	5.1
조직유형	선사	2	1.1
	터미널 및 운영사	82	46.3
	종합물류기업	23	13
	물류정보기술관련기업	59	33.3
	기타	11	6.2
직급	실무자	141	79.7
	단위부서 책임자급	30	16.9
	임원급	7	3.4
근무 년 수	1년 미만	20	11.3
	1년 이상~3년 미만	20	11.3
	3년이상 ~7년 미만	21	11.9
	7년 이상~10년 미만	22	12.4
	10년 이상	94	53.1
종업원 수	100명 이하	25	14.1
	300명 이하	63	35.6
	1000명 이하	87	49.2
	1000명 이상	2	1.1

2. 측정모형의 신뢰성과 집중타당성

본 연구에서는 확인적 요인분석을 통해 측정 하부모형의 신뢰성을 평가하기 위한 합성개념 신뢰도와 평균분산추출, Cronbach-α값을 검정하였으며, 그 결과는 다음의 <표 3>과 같다.

<표 3> 집중타탕성과 신뢰성 분석

요인	항목		집중타당성					내적신뢰성
		비표준화 추정치	표준화 추정치	t-값	측정오차	합성개념 신뢰도	AVE	cronbach-α
정보보안인식 (SA)	SA1	0.94	0.82	15.32	0.32	0.94	0.8	0.89
	SA2	1.00	0.92	-	0.15			
	SA3	0.83	0.89	19.63	0.21			
	SA4	0.88	0.94	22.07	0.11			
정보보안태도 (AT)	AT1	0.97	0.81	10.61	0.35	0.85	0.59	0.77
	AT2	0.98	0.78	10.26	0.39			
	AT3	1.00	0.77	-	0.41			
	AT4	0.87	0.72	9.41	0.48			
자기효능감 (SE)	SE1	0.99	0.92	21.92	0.16	0.94	0.79	0.89
	SE2	1.00	0.95	-	0.10			
	SE3	0.88	0.86	18.15	0.26			
	SE4	0.84	0.83	16.52	0.32			
규범신념 (SB)	SB1	1.00	0.93	-	0.14	0.91	0.78	0.88
	SB2	0.96	0.93	20.34	0.13			
	SB3	0.83	0.78	14.15	0.39			
사회적영향 (SI)	SI1	1.00	0.92	-	0.16	0.94	0.85	0.92
	SI2	0.96	0.93	20.91	0.13			
	SI3	1.00	0.91	19.70	0.17			
정보보안정책 준수 (SPO)	SPO1	1.00	0.95	-	0.09	0.93	0.78	0.88
	SPO2	0.99	0.93	23.51	0.13			
	SPO3	0.97	0.78	14.50	0.40			
	SPO4	0.95	0.86	18.35	0.27			

먼저, 각 구성개념들에 대하여 지정된 예측변수가 그들 구성개념을 충분히 설명하고 있는가를 확인하는데 필요한 추정치는 합성개념 신뢰도와 평균분산추출 값(Average Variance Extracted: AVE)이다. 먼저 합성개념 신뢰도의 경우 모든 구성개념이 권장수준인 0.7이상을 상회하는 것으로 나타나 전반적으로 양호한 수준으로 평가되었다. 그 중에서 정보보안인식, 사회적 영향, 자기효능감이 0.94로 가장 높았으며, 다음으로 정보보안정책 준수는 0.93, 규범신념이 0.91, 정보보안태도가 0.85로 전반적으로 합성개념 신뢰도가 높은 것으로 확인 하였다. 다음으로 평균분산추출 값의 경우에 구성개념에 의해서 설명되는 분산의 양을 나타내며, 0.5보다 작은 경우에는 측정오차가 구성개념에 의

해서 설명되는 분산보다 크기 때문에 신뢰성이 없다고 할 수 있다. 사회적영향이 0.85로 추정치가 가장 높게 나타났으며 그 다음으로 정보보안인식이 0.803으로 나타났다.

집중타당성의 분석은 측정모델의 요인 적재값과 t-값에 따라서 검정되며, 각 항목의 추정치가 0.5이상이며, 그 추정치의 t-값이 2.0 이상일 때, 측정항목의 집중타당성이 있는 것으로 판단한다. <표 3>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. 또한 내적신뢰도 Cronbach-α값 권장기준 0.7 이상의 수용기준에 부합되고 있어 측정항목의 구성개념에 대한 신뢰성이 확보되었음을 알 수 있다.

3. 측정모형의 판별타당성

본 연구에서의 판별타당성은 <표 4>에서 보는 바와 같이 각 구성개념들의 평균분산추출 값(AVE)의 제곱근이 다른 구성개념들 간의 상관계수보다 상회하고 있다. 이는 하나의 구성개념 내의 평균분산추출 값이 다른 구성개념과 공유하는 분산보다 크다는 것으로 변수간의 판별타당성이 있음을 확인할 수 있다.

<표 4> 변수간 상관계수와 AVE의 제곱근 값

변수	추출된 평균분산의 제곱근 값					
	1	2	3	4	5	6
1. 정보보안인식	**(0.90)**					
2. 정보보안태도	0.43	**(0.77)**				
3. 자기효능감	0.32	0.68	**(0.92)**			
4. 규범신념	0.18	0.19	0.46	**(0.88)**		
5. 사회적 영향	0.23	0.22	0.37	0.66	**(0.89)**	
6. 정보보안정책 준수	0.33	0.39	0.50	0.34	0.41	(0.88)

주: ( )는 각 변수의 AVE 제곱근.

4. 측정모형과 구조모형의 적합도 평가

본 연구의 측정모형과 구조모형에 대한 적합도 지수는 아래의 <표 5>와 같다. 먼저 측정모형을 살펴보면 χ^2(p)은 377.75(0.00)이며, χ^2을 자유도로 나눈 비율이 1.98로 권

장수준(≤3.00)에 부합하였다. 구조모형에서도 χ^2(p)은 469.91(0.00)이며, χ^2을 자유도로 나눈 비율이 2.38로 권장수준(≤3.00)에 부합하였다. GFI는 측정모형이 0.85, 구조모형이 0.82로 권장수준인 0.90보다 약간 낮게 분석되었지만 AGFI가 0.80에 근접하고 있으며, RMSEA 값은 측정모형과 구조모형 모두가 0.80으로 나타났다. 또한 IFI, CFI가 각각 측정모형이 0.95, 구조모형이 0.93이며, PGFI가 측정모형과 구조모형 모두 0.64이고 PNF가 0.75 등 수용기준을 상회하는 것으로 나타나 대체적으로 측정모형의 적합도가 수용기준을 충족하는 것으로 평가하였다. 또한 구조모형 적합도 역시 연구 개념들 사이의 관계를 설명하는데 적절한 것으로 판단하였다.

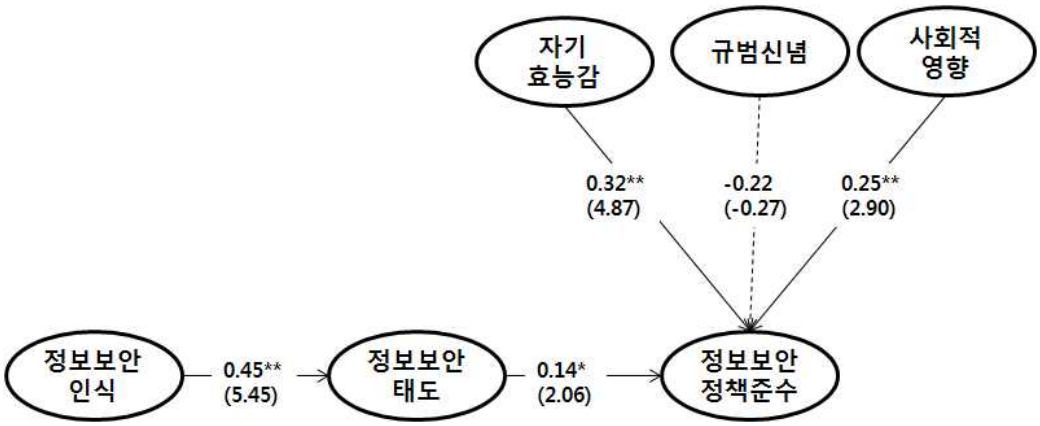
<표 5> 적합도 지수

구분	적합도지수	수용기준	측정모형 분석결과	구조모형 분석결과
절대 부합 지수	χ^2/df	≤3.00	1.98	2.38
	χ^2 자유도(df) p-value	≥0.05	377.75 191 0.00	469.91 197 0.00
	기초부합지수(GFI)	≥0.90	0.85	0.82
	근사원소평균자승잔차(RMSEA)	≤0.08	0.08	0.08
증분 부합 지수	수정부합지수(AGFI)	≥0.80	0.80	0.77
	표준부합지수(NFI)	≥0.90	0.90	0.88
	관계부합지수(RFI)	1.0근사	0.88	0.86
	증분부합지수(IFI)	1.0근사	0.95	0.93
	비교부합지수(CFI)	≥0.90	0.95	0.93
간명 부합 지수	간명기초부합지수(PGFI)	≥0.60	0.64	0.64
	간명표준부합지수(PNFI)	≥0.60	0.75	0.75

5. 가설검정 및 결과분석

구조모형의 분석결과에 따라 각 경로의 추정치와 t-값은 아래의 <그림 2>와 같이 나타났으며, 규범신념에서 정보보안정책 준수에 이르는 경로를 제외한 다른 모든 경로는 통계적으로 유의한 것으로 확인되었다.

<그림 2> 연구모형 검증결과



주) *:p<.05, **:p<.01 에서 유의함.

정보보안인식이 정보보안태도에 미치는 영향을 평가하기 위해 설정한 연구가설1(H1)은 경로계수가 0.45로 나타났으며, t-값이 5.454로 유의수준 p<0.01에서 통계적으로 유의한 것으로 나타나 가설이 채택되었다. 또한 정보보안태도가 정보보안정책 준수에 영향을 미친다는 연구가설2(H2)도 경로계수가 0.244이며, t-값이 2.06으로 유의수준 p<0.05에서 통계적으로 유의한 것으로 나타나 채택되었다. 자기효능감이 정보보안정책 준수에 영향을 미친다는 연구가설3(H3), 사회적 영향이 정보보안정책 준수에 영향을 미친다는 연구가설5(H5)도 유의수준 p<0.01에서 통계적으로 유의한 값을 보여 가설이 채택되었다. 그러나 규범신념이 정보보안정책 준수 영향을 미친다는 연구가설4(H4)의 경우에는 경로계수가 -0.22이며, t-값이 -0.27로 유의수준 p<0.05에서 통계적으로 유의하지 않은 값으로 나타나 기각하였다. 연구가설 검증결과는 아래의 <표 6>과 같다.

가설검정 결과를 바탕으로 본 연구의 결과를 분석하면 다음과 같다.

첫째, 해운항만조직 구성원들의 정보보안인식 정도가 높을수록 정보보안태도가 높게 형성되고 있음을 알 수 있다. 해운항만조직 구성원들이 개인의 신상정보, 패스워드, 프로그램, 데이터에 대한 보안의 중요성을 높게 인식할수록 컴퓨터 안정성 검증, 보안프로그램의 업데이트, 스팸메일 필터링, 주기적 패스워드 변경 등을 함에 있어서 긍정적인 태도를 가지고 있음을 알 수 있다.

둘째, 정보보안태도가 높을수록 정보보안정책 준수의 정도도 높게 나타났다. 해운항

만조직 구성원들이 정보보안을 위해 가지는 호의적인 태도, 즉 컴퓨터 안정성 검증, 보안프로그램의 업데이트, 스팸메일 필터링, 주기적 패스워드 변경을 하는 것이 호의적일수록 정보보안활동의 실제 적용의도, 이행의도, 조사의도, 보안활동 효과 의도가 긍정적임을 알 수 있다.

셋째, 해운항만조직 구성원들이 가지고 있는 자기효능감과 사회적 영향이 높을수록 정보보안정책의 준수사항을 호의적으로 받아들이고 있음을 알 수 있다. 해운항만조직에서는 구성원들이 정보보안정책에 대해 인지하고, 습득하고, 적용 및 적응하는 정도가 높을수록 정보보안정책에서 규정하고 있는 사항들이 잘 준수되고 있음을 알 수 있다. 또한, 해운항만조직 구성원들은 정보보안정책을 준수함에 있어서 사회적 인지도, 평가, 유행, 권유 등에 영향을 받고 있음을 알 수 있다.

넷째, 해운항만조직 구성원들은 규범신념에 따라 정보보안정책 준수의 정도가 큰 영향을 받지 않는 것으로 나타났다.

<표 6> 연구가설 검증결과 요약

연구가설	경로계수	t-값	검정결과
[H1] 정보보안인식은 정보보안태도에 정(+)의 영향을 미친다.	0.45	5.45**	채택
[H2] 정보보안태도는 정보보안정책 준수에 정(+)의 영향을 미친다.	0.14	2.06*	채택
[H3] 자기효능감은 정보보안정책 준수에 정(+)의 영향을 미친다.	0.32	4.87**	채택
[H4] 규범신념은 정보보안정책 준수에 정(+)의 영향을 미친다.	-0.22	-0.27	기각
[H5] 사회적 영향은 정보보안정책 준수에 정(+)의 영향을 미친다.	0.25	2.90**	채택

Ⅴ. 결 론

조직구성원들에게 정보보안의 위험성과 업무를 수행함에 있어 불확실성에 항상 노출되어 있는 상태의 정보시스템을 다루고 있다는 것을 확인시켜주는 것은 인지적인 차원으로 쉬운 문제가 아니다. 하지만 조직에서 적극적인 정보보안 관련 이슈에 대해 관심을 가지고 조직구성원들을 정보보안 관점에서 어떻게 인도할 것인가를 구체적으로 모색하여 조직구성원에게 정보보안의 중요성을 인식시키는 것이 무엇보다 중요하다. 이를 위해 조직에서는 정보보안을 관리할 수 있는 지침과 규정을 동반한 정보보안정책이라

는 가이드라인이 존재한다. 조직구성원이 모든 사항을 다 이해하고 보안정책 사항을 잘 준수하였을 때는 별다른 정보보안 위험의 정도가 심각하게 받아들여지지 않는 상황으로 이해될 수 있으나, 조직구성원들이 보안정책 내부의 사항들 중 무시해 버리는 정책사항이나, 보안정책관련 권고내용을 위반하거나 잘 알지 못한 상태에서는 정보보안 위험의 정도가 심각한 상황으로 받아들여지는 것이 당연한 사실이다.

해운항만조직에서의 정보의 중요성은 시간이 지날수록 커지고 있다. 물리적인 물류의 흐름은 정보의 흐름으로 대변되고 있다. 어떤 조직보다도 해운항만조직에서는 수많은 정보들이 EDI, RFID, 스마트폰 등과 같은 정보기술을 통해 실시간으로 이동되고 있다. 따라서 본 연구에서는 보다 발전적이며 실제적으로 적용 가능한 해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인을 파악하고자 하였다. 이를 위하여 먼저 정보보보안인식과 정보보안태도와의 관계를 살펴보았고, 다음으로 정보보안태도와 정보보안정책 준수와의 관계를 살펴보았다. 또한 정보보안정책 준수의 선행요인으로 자기효능감, 규범신념, 사회적 영향 변수를 설정하여 연구모형을 설정하였다.

본 연구결과를 요약하면 다음과 같다.

첫째, 해운항만조직 구성원들의 정보보안인식 정도가 높을수록 정보보안태도가 높게 형성되고 있음을 알 수 있었다. 또한, 해운항만조직 구성원들이 정보보안을 위해 가지는 태도가 호의적일수록 정보보안정책에서 규정하고 있는 준수사항을 실제로 적용하고, 이행하고, 효과적으로 활용하는 정도가 높게 나타났다. 따라서 해운항만조직에서는 구성원들의 정보보안정책 준수 정도를 높이기 위해 정보보안인식 정도와 정보보안태도가 높게 형성될 수 있기 위한 방안을 모색해야 할 것이다. 이와 관련된 선행연구에서는 정보보호의 중요성을 확산시키고 정보보호를 담당하는 교육의 중요성을 강조하였으며, 정보보호인력의 질적 양성을 위해 보다 체계적인 교육과정의 필요성을 높이 인식하고, 정보보호 전문 인력이 갖추어야할 지식 및 기술에 대해 강조하고 있다(유혜원 등, 2009).

둘째, 해운항만조직에서는 구성원들이 정보보안정책에 대해 인지하고, 습득하고, 적용 및 적응하는 정도가 높을 경우 정보보안정책에서 규정하고 있는 사항들이 잘 준수되고 있음을 알 수 있었다. 또한, 해운항만조직 구성원들은 정보보안정책을 준수함에 있어서 사회적 인지도, 평가, 유행, 권유 등 사회적 영향을 받고 있음을 알 수 있었다.

셋째, 해운항만조직 구성원들은 규범신념에 따라 정보보안정책 준수의 정도가 큰 영향을 받지 않는 것으로 나타났는데 이와 같은 결과를 보인 이유를 분석하면 다음과 같다. 조직의 적절한 정보보호정책수립 및 실행은 조직의 내재적인 가치 및 경쟁력을 증가시키는 역할을 할 수 있도록 규범적 신념을 형성하도록 한다(Siponen, 2000). 조직구성원의 정책관련 규범에 대한 신념도가 높을수록 보안정책을 잘 준수하기 위한 행동이 나타난다고 할 수 있다. 그런데 해운항만조직에서는 규범신념이 정보보안정책 준수에

통계적으로 영향이 없다는 사실은 현재 해운항만조직에서는 구성원들이 정보보호정책에 대한 규범신념을 형성할 수 있는 분위기를 잘 형성하지 못하고 있음을 반영한 결과로 해석될 수 있다. 따라서 해운항만조직에서는 구성원들이 정보보안정책의 규정을 잘 준수할 수 있게 하기 위하여 정보보안정책의 안전성, 신뢰성, 우수성, 적용성을 높일 수 있는 규범신념을 형성하도록 노력해야 할 것이다.

본 연구의 의의는 다음과 같다.

첫째, 해운항만조직 구성원들의 정보보안정책에 관한 중요성을 일깨워주는 조직구성원의 개인에 대한 인식을 파악할 수 있도록 실증적으로 검증하였다는 점이다.

둘째, 측정대상이 실무자가 79.8%의 비율을 차지하고 있어서 조직 내 정보보안에 관해 실무적으로 활용될 수 있는 정보보안정책 준수 요인을 도출할 수 있었다.

셋째 시간이 지날수록 정보보안의 중요성이 커지고 있는 해운항만조직 구성원들의 정보보안정책 준수 정도를 파악하여 해운항만조직의 정보보안정책 수립 시 참고할 수 있는 기반을 제공하였다.

본 연구는 위와 같은 학문적, 실무적 기여가 있음에도 불구하고 다음과 같은 한계점을 갖고 있다. 첫째, 정보보안정책 규범신념과 정보보안정책 준수 간의 관계가 유의하지 않게 나온 것은 정보보안정책 규범신념이 조직 내에서 이행되고 활용될 수 있을 정도로 정보보안에 큰 영향력을 나타내는 요인이 아니라는 것이다. 향후의 연구에서는 조직의 정보보안에 대한 개인의 위험에 대한 인식분야를 측정하여 정보보안위험과 보안정책의 신념 간의 관계를 분석해서 어떠한 관련성이 있는지 살펴볼 필요성이 있다. 둘째, 본 연구에서 측정하고자 하는 정보보안정책 준수가 해운항만조직을 대상으로 국한되어 분석하였기에 해운항만분야 이외의 조직의 특성에 따른 정보보안정책 준수에 영향을 미치는 요인을 비교·분석하는 연구가 이루어져야 할 것이다.

참고문헌

노민선·이삼열, “중소기업의 산업보안 역량에 대한 영향요인 평가”, 『한국행정학보』, 제44권 제3호, 2010, 239-259.

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

디지털데일리, “2011년은 데이터 유출의 해, 트렌드마이크로 연간보고서 발표”, 2012. 1. 26.

박준경·김범수·조성우, “기업 정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인”, 『경영학연구』, 제40권 제4호, 2011, 955-985.

부산일보, “부산신항 배후단지 물류 정보 한 손에”, 2010. 8. 11.

유혜원·김태성·전효정, “정보보호분야 지식 및 기술수요”, 『정보보호학회지』, 제19권 1호, 2009, 23-28.

임채호, “효과적인 정보보호인식 제고방안”, 『정보보호학회지』, 제16권 제2호, 2006, 30-36.

장명희, “해운・항만기업 정보시스템 리스크요인에 대한 발생가능성, 영향력 분석과 상대적 중요도 평가”, 『해운물류연구』, 제25권 제1호, 2009, 57-82.

전자신문, “내부정보 유출 막아라, 기업들 비상, 해결책은?”, 2011. 9. 7.

정보통신부, 『국가정보보호백서』, 2010.

Ajzen, I. and Fishbein, M., “Attitude-Behavior Relation: A Theoretical Analysis and Review of Empirical Research,” *Psychological Bulletin,* Vol.84, No.5, 1997, 888-918.

Amitava, D. and McCrohan, K., “Management's Role in Information Security in a Cyber Economy,” *California Management Review,* Vol.45, 2001, 67-87.

Bandura, A., “Self-Efficacy: Toward a Unifying Theory of Behavioral Change,” *Psychological Review,* Vol.84, 1977, 191-215.

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.

Carrie M. and Rebecca, T. F., “You are the Key to Security: Establishing a Successful Security Awareness Program,” *ACM SIGUCCS Conference*, Vol.32, 2004, 346-349.

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

Davis, F., “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology,” *MIS Quarterly*, Vol.13, No.3, 1989, 319-340.

Eagly, A. H. and Chaiken, S., *The Psychology of Attitudes,* Harcourt Brace Javanovich College Publishers, 2006.

Gist, M. E., “Self-efficacy: Implications for Organizational Behavior and Human Resource Management,” *Academy of Management Review,* Vol.12, No.3, 1987, 472-485.

Goodhue, D. L. and Straub, D.,W., "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures," *Information & Management*, Vol.20, 1991, 13-27.

Halibozek, E. and Kovacich, G, L,. *Mergers and Acquisitions Security, Corporate Restructuring and Security Management,* Butterworth-Heinemann, 2005.

Jeffrey, M. S., Kathryn. R. S., and Paul M., "Analysis of End User Security Behavior," *Computers & Security,* Vol.24, 2005, 124-133.

Johnston, A. C. and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly,* Vol.34, No.3, 2010. 549-566.

Knapp, M., Chisholm, D., Leese, M., Amaddeo, F. and Tansella, M., "Comparing Patterns and Costs of Schizophrenia Care in Five European Countries: the EPSILON Study. European Psychiatric Services: Inputs Linked to Outcome Domains and Needs," *Acta Psychiatr Scand*, Vol.105, 2002, 42-54.

Rice, R E. Gr., Schmitz, A. E. and Torobin, J., "Individual and Network Influences on the Adoption and Perceived Outcomes of Electronic Messaging," *Social Networks*, Vol.12, No.1, 1990, 27-55.

Rundmo, T. and Sjoberg, L., "Risk Perception by Offshore Oil Personnel During Bad Weather Conditions," *Risk Analysis,* Vol.18, No.1, 1998, 111-118.

Russell, D. and Gangemi, G., *Computer Security Basics*, O'Reilly & Associated, 1991.

Siponen, M., "Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice," *Information Management and Computer Security*, Vol.8, No.5, 2000, 197-209.

Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J., "An Analysis of End User Security Behaviors," *Computers and Security,* Vol.24, 2005, 124-133.

Straub, D. W. and Welke, R. J., "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, Vol.22, 1998, 441-469.

Thomas, K. and Velthouse, B., "Cognitive Elements of Empowerment: An "Interpretive" Model of Intrinsic Task Motivation," *Academy of Management Review*, Vol.15, 1990, 666-681.

Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D., "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, Vol.27, No.3, 2003, 425-478.

국문요약

해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인

강다연 · 장명희

정보기술의 발전은 기업에게 많은 이익을 가져다주었지만, 정보유출이라는 심각한 문제를 야기하고 있다. 이에 따라 기업들은 정보보안을 위해 정보보안정책을 수립하고 조직구성원들이 정보보안정책을 준수할 것을 요구하고 있다. 본 연구에서는 해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인들을 실증분석 하기 위해 정보보안인식, 정보보안태도, 자기효능감, 규범신념, 사회적 영향들을 영향요인으로 선정하였다. 분석결과에 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. 하지만 규범신념과 정보보안정책 준수와의 관계는 유의하지 않은 것으로 분석되었다. 본 연구의 결과는 정보유출문제가 발생할 가능성이 큰 해운항만조직의 구성원들이 정보보안정책의 준수사항을 어느 정도로 받아들이는 지를 확인함으로써 해운항만조직에서 정보보안과 관련된 정책을 수립하는데 기반을 제공할 것으로 기대한다.

핵심 주제어 : 해운항만조직 구성원, 정보보안인식, 정보보안태도, 정보보안정책 준수