JFMSE, 29(4), pp. 1032~1042, 2017.
수산해양교육연구, 제29권 제4호, 통권88호, 2017.
www.ksfme.or.kr
http://dx.doi.org/10.13000/JFMSE.2017.29.4.1032

항만물류분야의 정보보호관리체계기반 정보보안시스템구축에 관한 연구

조 규 성†
(동명대학교)

Improvements of Security System based on Port Logistics Information System

Gyu-Sung CHO†
(TongMyong University)

Abstract

Port logistics is an important industry that conducts the import and export functions of a company, therefore various information pertaining to port logistics should be intensively managed. However, there have been insufficient efforts to secure various logistics information in the port logistics industry from external threats. So it needs to manage the port logistics information system to protect and build a security management system for integrated logistics information. It is necessary a new system to secure various logistics information in the port logistics industry from external threats. In this paper, we have developed a new diagnostic system which is a information security management system (ISMS) based on the port logistics information system to decrease the vulnerabilities. This suggested system can analyze vulnerabilities of port logistics information system and show the best solutions to protect the system from security defects.

Key words : Port Logistics, Information System, Information Security Management System, Improvements

Ⅰ. 서 론

IT 기술을 기반으로 한 정보기술 발전은 우리 사회를 지식정보사회로 변화시켰고, 이로 인해 국내외 어디에서나 지식과 정보를 인터넷 등을 통해서 공유할 수 있게 되었다. 결국 정보기술 개발 및 공유는 각 나라를 정보화 사회로 이끄는 계기가 되었다. 그 결과 정보기술 발전은 기업의 정보시스템 경쟁력 강화를 위해 보다 많은 투자를 하게 되는 원인이 되기도 하였다. 하지만 현재까지 많은 기업에서는 다양한 정보시스템을 개발하고 관련 기능 향상을 위한 많은 노력을 수행하고 있으나, 개발된 정보시스템에서 사용되는 중요 정보를 대내외적으로 보호하기 위한 필요성 인식 및 노력은 부족한 상황이다(Ko 2016, Won et al., 2015). 또한 기업에서 운영되고 있는 정보시스템의 예기치 못한 침해사고나 내부인에 의한 보안 사고는 기업의 운영 및 경영에 큰 위험과 막대한 손실을 끼칠 수 있으나, 많은 기업에서는 이러한 상황의 중요성을 인식하지 못하고 있는 것이 현실이다. 기업의 인식 부족은 결국 기업이 보유한 중요 정보의 불법적인 외부 유출 및 기업

† Corresponding author : 051-629-1466, gscho@tu.ac.kr.
※ 이 논문은 2016년도 동명대학교 교내학술연구비 지원에 의하여 연구되었음(2016A022).

운영에 심각한 영향을 미치게 되었다. 따라서 해킹 등을 통한 기업 정보의 누출사고 등으로 인해 국내에서도 기업의 중요 정보를 보호하기 위한 노력의 일환으로 정보보호관리체계 (ISMS : Information Security Management System)를 도입하여 적용하고 있다. 정보보호관리체계는 정보 통신 서비스 제공자가 정보통신망의 안정성 및 신뢰성을 확보하여 정보 자산의 기밀성, 무결성, 가용성을 실현하기 위한 관리적·기술적 수단과 절차 및 과정을 체계적으로 관리 및 운용할 수 있는 체계이다. 정보보호관리체계는 2010년부터 국내에 적용되고 있으며, 금융 산업 등을 중심으로 2017년 2월 기준 436곳에 정보보호관리체계가 적용되어 운영되고 있다. 하지만 정보보호관리체계는 금융권 및 인터넷 운영 기업체 등의 일부 IT 기반 산업에 국한되어 적용되고 있어 지속적으로 다양한 산업으로의 확대가 필요한 상황이고, 최근에는 항만물류분야에 대한 적용의 필요성이 제기되고 있다(Ko, 2016).

항만물류산업에서는 미국의 9·11 테러사건 발생으로 인해 물류보안 관련 규제 및 보안제도를 강화하게 되었고, 항만물류산업 특성상 국가간 무역으로 국가 간 보안협력이 매우 중요하게 되었다(Korea Maritime Institute, 2009). 이로 인해 항만물류산업은 물류흐름의 효율성뿐만 아니라 보안관련 신기술의 적용 및 보안장비의 투입 등을 통한 항만물류분야의 보안체계 구축에 많은 노력이 필요할 것으로 예상 되고 있다. 현재 항만물류분야에서 보안강화를 위한 노력으로 컨테이너 및 화물 스캔 운영시스템 도입, 보안시설에 대한 외부인 출입관리시스템 구축, 무선인식기술 기반 실시간 모니터링시스템 도입 및 운영, 불법침입 탐지 시스템 등의 물리적 보안시스템이 적용되어 운영되고 있다. 특히 항만물류산업의 대표적 시설인 항만컨테이너터미널은 제1급지 국가보안시설로 지정될 만큼 중요 보안시설로서 다양한 물리적 보안시스템이 도입되어 운영되고 있다. 그 이유는 항만컨테이너터미널에서 정보보안에 대한 문제가 발생하여 항만컨테이너터미널이 운영되지 못할 경우에는 국내의 수출과 수입 업무가 마비되는 초유의 상태까지 발생될 수 있기 때문에 항만물류산업의 정보보안은 어느 산업 못지않게 중요하다. 하지만 현재 항만컨테이너터미널은 물리적 보안 위주로 구축되어 운영되고 있고, 소프트웨어 측면에서의 정보보호를 위한 정보보호관리체계 구축 등의 노력은 상대적으로 미비한 수준에 있다(Won et al., 2015).

국내에서는 금융권 등을 중심으로 기업의 정보를 효율적으로 보호하기 위한 정보보호관리체계 구축 및 적용에 관한 연구가 수행되고 있으며, 최근에는 정보보호관리체계를 금융권 이외의 다양한 산업에 적용하려는 연구를 수행하고 있다.

Jung et al., (2011)은 항공기반시설에서 발생될 수 있는 보안사고 대응을 위한 정보보호관리체계를 설정하고 항공기반시설에서 요구되는 보안 충족 가능 여부를 평가하고 분석할 수 있는 정보보안관리체계 프레임워크를 제시하였다. Jeong & Ahn(2012)는 교육환경에 적합한 정보보호관리체계 모델을 개발 및 적용함으로써 교육환경의 정보보호 수준을 제고하고, 정보보호 관리 노력의 방향성과 향상 방안을 제시하였다. Kim & Kim(2012)는 미국 스마트 그리드 제도와 비교 분석을 통해 현재 국내에서 시행되고 있는 정보보호관리체계기반의 한국형 스마트 그리드를 수행하기 위한 평가기준을 제시하였다. Lee et al. (2013)은 정보보호관리체계와 역량성숙도모델통합을 통해 의료정보보호관리기준, 의료정보보호관리 프로세스, 의료정보보호관리 프로세스 성숙수준으로 구성된 의료정보보호관리체계를 제시하였다. Min(2012)은 우리나라의 물류보안의 현황과 대처에 관한 문제를 제시하였고, Kang(2013)은 항만물류보안관리 시스템의 체계화 및 일원화 방안을 제시하였으나 항만물류산업에 맞는 정보보호관리체계 개발 및 적용에 관한 연구는 전무한 상황으로 단편적인 보안 개선 방안과 국내 보안 관련 현황만 제시하고 있다.

이에 본 연구는 항만물류산업의 정보보호 강화를 위한 기초연구로 항만물류분야에 적합한 정보보호관리체계 구축 및 개선에 관한 연구를 수행하고자 한다. 이를 기반으로 도출된 연구결과는 국내 항만물류산업의 정보보호 강화를 위한 운영방안의 기초 자료로 활용될 수 있을 것이다. 이를 위해 본 연구에서는 제Ⅰ장은 서론, 제Ⅱ장은 정보보호관리체계 정의 및 국내 운영 현황, 제Ⅲ장은 항만물류정보보안 운영 현황, 제Ⅳ장은 항만물류정보보호 관리체계 구축 방안 제시 및 제Ⅴ장은 본 연구의 결론을 제시하였다.

Ⅱ. 정보보호관리체계 정의 및 운영

1. 정보보호관리체계 도입 배경

과거에는 특정 제품이나 기업체내 일부 부서를 중심으로 정보보호 활동이 수행되어 기업 내 전부서에서 요구되는 정보보호 수준을 만족시키기에는 많은 한계가 있었다. 이로 인해 국내에서도 단편적이며 부분적인 정보보호를 벗어난 보다 높은 수준의 기업체 정보보호관리 활동을 수행하기 위한 정보보호관리체계 구축 및 적용이 요구되었다. 기업의 정보보호는 단순히 기업체 운영에서 발생되는 운영비용이 아니라 비즈니스 기회 예측 및 위험에 적절히 대응하는 핵심경쟁력으로 예상하지 못한 위기상황에서 비즈니스 안정성을 유지하고 정보자산을 적절하게 보호하기 위한 경영활동의 일부가 되기 때문에 정보보호관리체계 도입이 필요하게 되었다(Kim et al., 2006).

2. 정보보호관리체계 정의

정보보호관리체계는 기업의 정보자산의 기밀성, 무결성, 가용성을 유지하면서 정보자산을 보호하고 조직의 사업 목적을 달성하고, 사업 수행

<Table 1> Main Composition of ISMS

Index	Control Area	Num. of Checklist
Processes of ISM	1. Setting the Establishment & Range of Information Security Policy	2
	2. Consist of the Responsibility of Board of Directors and Organizations	2
	3. Risk Management	3
	4. Suggesting the Alternatives of Information Security	2
	5. Follow-up Management	3
	Subtotal	12
Measures of Information Security	1. Police of Information Security	6
	2. Organization of Information Security	4
	3. Security for Outsider	3
	4. Sorting for Information Assets	3
	5. Education for Information Security	4
	6. Human Security	5
	7. Physical Security	9
	8. Security for System Development	10
	9. Password Control	2
	10. Access Control	14
	11. Operation Security	22
	12. Management for Attacking Accident	7
	13. IT Disaster Recovery	3
	Subtotal	92
Total		104

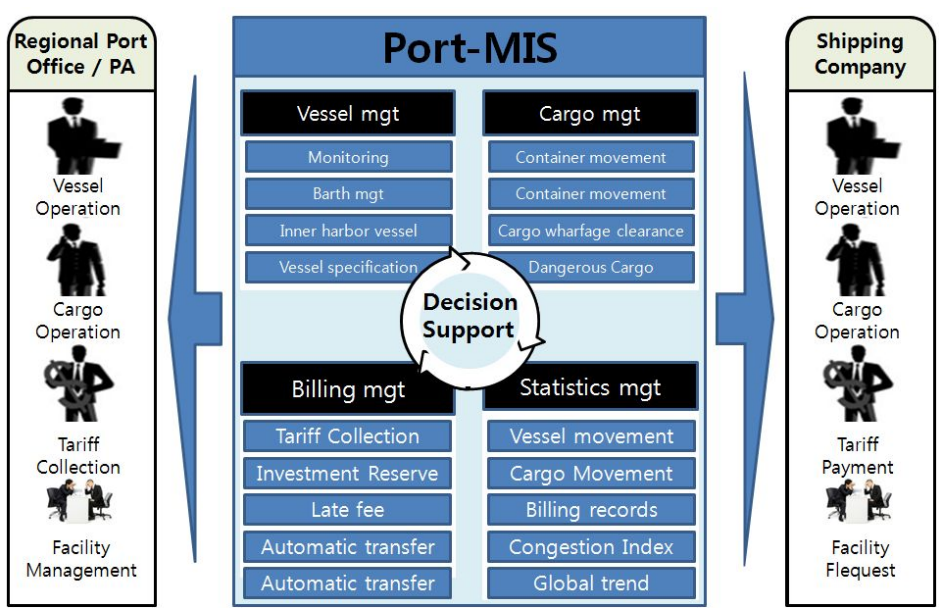
Source: Korea Internet & Security Agency

하기 위한 경영관리 체계 중의 하나로 정보자산의 보호에 관련된 정책 및 대책을 수립·관리·운영하는 종합적인 체계이다(Ko, 2016). 정보보호관리체계는 미래창조과학부에서 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 기업체들을 대상으로 정보보호관리에 적합한지를 평가하여 주어진 요건에 따른 기업체에게 부여하는 인증이다.

3. 정보보호관리체계 구축

정보보호관리체계 인증기준은 정보보호 관리과정과 정보보호대책으로 구성되어 있고 정보보호관리과정은 관리체계의 메인프레임으로서 전반적인 관리체계 운영 라이프사이클로 구성되어 있다. 정보보호관리체계로 구축되기 위해서는 정보보호대책 13개 분야 92개 통제사항 등 총 104개 통제사항에 대한 내용을 구성해야 된다. <Table 1>은 정보보호대책 13개 분야에 대한 인증기준을 제시하고 있다. 제시된 인증기준의 적합성 유무에 따라 각 분야별 (정책, 조직, 교육 등 관리적 부문과 개발, 보안통제, 운영 통제 등 물리적·기술적 부문에 대한 정책, 준수 및 검토 등) 관리·운영에 대한 세부항목으로 구성하고 있다.

현재까지 국내에 많은 기업들이 정보보호관리체계를 도입하여 구축하고 있는 이유는 단순한 정보보안 개념에서 벗어나 조직적이고 종합적인 정보보호 대책을 구현함으로써 기업의 정보보호 관리 수준을 향상 시킬 수 있기 때문이다. 뿐만 아니라 최근에 급증하고 있는 다양한 형태의 해킹, DDos (Distributed Denial of Service) 등의 침해 사고 발생 시 신속하게 대응 및 관련 피해를 최소화 할 수 있기 때문이다. 또한 경영진 차원에서의 상시 모니터링 체계구축이 가능하고, 경영진이 직접 정보보호 의사결정지원에 참여함으로써 기업은 사이버 침해사고에 효율적으로 대처가 가능하기 때문이다.



Source: Ministry of Oceans and Fisheries

[Fig. 1] Concept of Port-MIS

Ⅲ. 항만물류정보 정의 및 운영기술 현황

1. 항만물류 정의 및 항만정보운영시스템 운영 현황

항만은 해운과 내륙운송을 연결하는 결절점으로서 제품생산, 물류 및 국제교역기능과 배후지의 경제발전을 위한 기지로서의 역할을 수행하는 종합적인 공간이며, 항만물류란 항만을 중심으로 수행하는 물류로 항만물류업무에서 발생되는 다양한 정보를 항만물류정보라고 한다. 우리나라에서 항만물류의 가장 중심적인 역할을 수행하고 있는 곳은 항만컨테이너터미널로서 해상/항만에서 발생되는 수출입화물의 물류흐름과 관련된 제반 업무를 수행하는 곳이다(Cho, 2015). 항만컨테이너터미널의 업무는 크게 해상수입업무, 해상수출업무 및 환적업무로 구분할 수 있다. 해상수입업무는 해외에서 수입된 화물을 선적한 선박이 항만에 도착하여 입항절차를 거쳐 화물을 하역하고 하역된 화물이 부두에서 장치/보관되거나 통관절차를 거쳐 항만 밖으로 반출되는 것이다. 해상수출업무는 수출화물이 내륙운송수단을 통해 항만에 도착하여 장치보관되었다가 선박에 선적되어 외국으로 반출되는 과정이며, 환적업무는 화물이 도착된 입항지에서 하역을 하여 반입, 반출된 후 곧바로 선적하여 출항하는 것이다. 국내에서는 다양한 항만물류 업무를 효율적으로 처리하기 위해서 그림 1과 같은 항만물류정보시스템 (Port-MIS : Port Management Information System)이 구축되어 운영되고 있다(KLNet, 2013).

항만물류정보시스템은 해양수산부에서 화주 및 항만운영사에게 항만물류의 다양한 정보 및 운영의 효율성 제공 목적으로 선박입출항관리, 항만시설사용 등을 지원하는 종합정보시스템이다. 현재 전국 28개 무역항에서 사용되고 있으며, 선박입출항, 화물, 항만시설 등에 대한 정보를 종합적으로 관리 및 관련 정보를 제공하고 있다. 국가차원에서 항만운영정보시스템을 구축한 목적은 종합물류비용 절감으로 문서 없는 행정체제 구현으로 방문처리에 따른 민원인의 불편 해소 및 대국민 서비스 제고 향상이다.

2. 항만물류보안 정의 및 기술현황

보안은 개인이나 기업을 대상으로 경보 등 각종 안전관련 서비스를 제공하는 목적으로 인력경비를 비롯해 시스템경비, 무인자동화 시스템, CCTV 및 도난방지시스템 등을 들 수 있다. 보안은 외부의 각종 위해로부터 개인의 이익이나 생명, 시설물 및 재산을 보호하는 것이 주요 목적이다. 이러한 보안개념을 항만물류에 접목한 항만물류보안은 항만컨테이너터미널을 통한 화물의 수출입과정에서 발생되는 업무에서 컨테이너 운송기사 확인 및 컨테이너 확인 과정, 적하목록신고서 작성 및 신고와 봉인된 Seal 확인 과정 등을 수행한다. 항만물류업무를 수행하는데 적용되고 있는 기술을 정리하면 크게 6가지로 구분할 수 있다(Korea Institute of Science Technology Evaluation and Planning, 2007).

1) 보관/하역기술은 보관/하역활동을 효율적으로 운영하기 위한 IT 신기술을 활용하여 무인, 고속, 대형하역 장비 등을 통해 물품의 하역을 효율화하는 기술이다.

2) 이송기술은 창고, 컨테이너장치장 등 제한된 보관 거점 내에서 물품을 효율적이고 경제적으로 이동시키는 제반 기술로서 Navigation System, Supervisor 및 무선통신시스템 요소 기술 등이 있다.

3) RFID기반 태그인식 기술은 컨테이너에 태그를 부착하여 무선으로 제품의 정보를 확인하고 주변 상황을 감지시켜 원하는 데이터를 처리하는 개체 인식 기술로서 적재패턴 및 태그 부착위치 선정, 태그의 유효한 정보체계관리 등이 있다.

4) 물류안전/보안 기술은 재무, 제조, 정보경영, 포장, 저장시설, 물류 등을 포함하는 조직과 제조, 서비스, 저장, 유통에 이르는 생산 혹은 공급망 단계에

관한 통합적인 물류 안전/보안기술을 말하고, 컨테이너 화물 보안을 위한 전자 Seal 및 화물 상태 확인을 위한 RFID기술 등이 있다. 뿐만 아니라 보안 관련 Image Processing 및 센서 기술로서 실시간 화물 흐름 파악 및 공급사슬망관리 관점에서 각 물류업체 간의 화물처리상태 추적 기술도 해당된다.

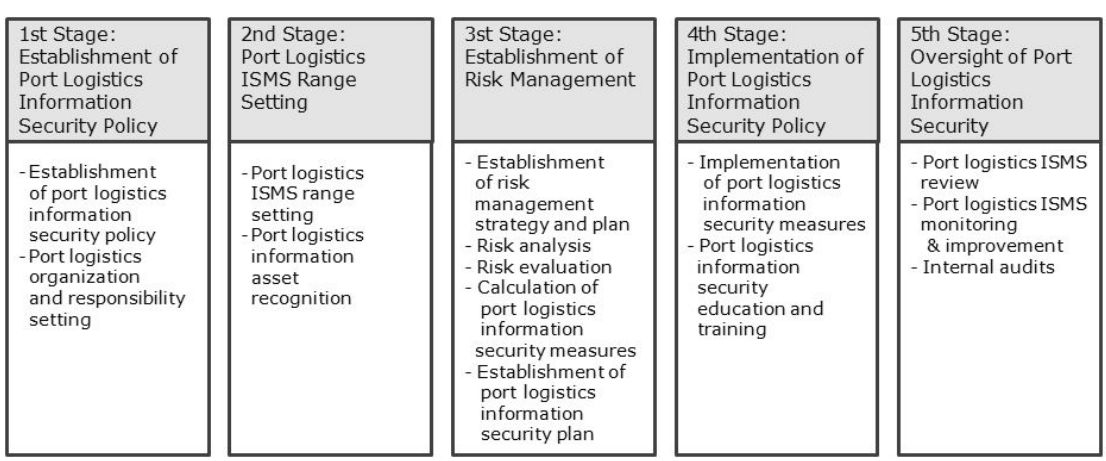
5) 물류인증기술은 국제규격의 물류 인증으로 ISO28000, C-TPAT (Customs-Trade Partnership against Terrorism), ISO14001:2004 등이 적용되고 있다.

하지만 국내 항만컨테이너터미널에서 수행되는 보안은 운송되는 화물에 대한 물리적 보안을 중심으로 수행되고 있으나, 항만물류정보시스템을 사용하는 화주나 항만운영사를 대상으로 물리적 보안중심의 정보보호가 아닌 시스템적 보안 업무를 중심으로 항만물류분야 맞춤형 정보보호관리체계 기반으로 운영되고 있지 못한 상황이다 (Korea Maritime Institute, 2009). 이로 인해 기업에서는 외부로의 해킹 등에 따른 상황에서 유연하게 대처할 수 있는 방안으로 항만물류분야에 특화된 정보보호관리체계를 제시하게 되었다.

Ⅳ. 항만물류분야 정보보호관리체계 구축 방안

본 연구는 항만물류산업에 맞는 정보보호관리체계 구축을 주요 목적 [Fig. 2]와 같이 총 5단계를 제시한다. 첫 번째 단계에서는 항만물류정보보호를 구축하기 위해서 요구되는 항만물류회사의 정보보호에 관한 주요 정책 방향을 수립한다. 두 번째 단계에서는 항만물류분야 정보보호체계 적용 범위를 설정한다. 세 번째 단계에서는 항만물류정보보안정책을 수립 후 발생 될 수 있는 정보보안에 관한 위험 분석 및 관리를 수행한다. 네 번째 단계에서는 항만물류정보보호의 개선 방안 등을 수립한다. 마지막 단계에서는 완성된 항만물류정보체계의 현장 적용에 대한 평가 수행 및 항만물류분야의 정보보호관리체계를 지속적으로 관리 및 감독을 수행한다.

항만물류분야의 정보보호관리체계를 구축하기 위해 제시된 5단계 절차를 수행하기 위해서 절차별 세부 통제분야를 <Table 2>와 같이 13개 통제분야로 구별하였고, 통제분야별 수행내용을 제시하였다. 예를 들어 통제분야 2의 항만물류정보보호부서를 신설할 경우에는 해당 부서의 회사 조직내 역할 및 책임 등에 대한 명확한 기준을 정립했다. 또한 통제분야 7의 물리적 항만물류보안을 위해서는 항만물류기업체서 운영되고 있는 보안시스템 및 사무실 등에 적용되고 있는 물리적 보안의 범위 및 수행 방안 등에 대해 제시했다.



[Fig. 2] Five-stage Management Procedure

<Table 2> Requirements of Port logistics ISMS

Control Area	Main Details
1. Port Logistics Information Security Policies	Admission and Publishing of Policies, Systemization of Policies, Maintenance of Policies
2. Port Logistics Information Security Organization	Systems, Responsibilities, and Roles of an Organization
3. External Security	Definition of Port Logistics Security Requirements and External Port Logistics Security Performance
4. Port Logistics Information Asset Classification	Port Logistics Information Asset Recognition and Responsibilities, and Information Asset Classification and Settlement
5. Port Logistics Information Security Education	Education Program Establishment, Education, and Evaluation
6. Manpower Reinforcement	Port Logistics Information Security Responsibilities and Personnel Regulations
7. Port Logistics Physical Security	Port Logistics Physical Security Area, System Security and Office Security
8. Port Logistics System Development Security	Analysis and Design of Port Logistics Security Management, Implementation and Security Transfer, Outsource Development Security
9. Password Control	Password Policies, Password Key Management
10. Access Control	Access Control Policies, Access Authentication Management, User Authentication and Recognition, Access Control Area
11. Port Logistics Operation Security	Operation Procedures and Adjustment Management, System and Service Operation Security, Electronic Transaction and Port Logistics Information Transmission Security, Media Security, Malware Management, Log Management and Monitoring
12. Invasion Accident Management	Procedure and System, Solutions and Recovery, Oversight of Port Logistics System
13. Port Logistics System Disaster Recovery	Port Logistics System Build, Implementation of Port Logistics Security Measures

그 이유는 항만물류업무를 수행하는 기업체는 화물 중심의 운영이 기본 원칙이기 때문에 원활한 화물의 운반 및 보관 등을 수행하기 위해서는 물리적 보안의 역할이 중요하기 때문이다.

이러한 일련의 통제 분야를 구체적으로 기술하면 다음과 같다.

(1) 항만물류정보시스템 정보보호정책 수립

항만물류분야 정보보호체계를 구축하기 위해서는 항만물류정보시스템의 정보보호정책을 수립한다. 정책을 수립하기 위해서는 정부에서 제시하고 공표하는 관련 법령 및 정책을 지속적으로 모니터링하고 관련 내용의 회사 정책에 반영해야 할 것이다. 현재 항만 경비 및 보안업무 관련 법령은 다음과 같이 정리할 수 있다.

대통령훈령에 따른 통합방위법·통합방위법시행령·통합방위지침, 국가대테러활동지침, 보안업무규정 및 보안업무규정시행규칙이 있다. 또한 국방부훈련에 따른 국가중요시설 지정 및 방호훈령과 국가정보원에 따른 국가보안목표관리지침, 해양수산부에 따른 국제항해선박 및 항만시설의 보안에 관한 법률·시행령·시행규칙이 있다.

또한 지역별 항만공사에 따른 항만공사 정관, 항만법 및 항만공사법, 지역별 항만부두출입증발급 및 출입자관리세부시행지침이 있으며, 경찰청에 따른 청원경찰법·시행령·시행규칙, 경비업법·시행령·시행규칙 및 경비업체보안업무관리규칙이 있다. 따라서 회사 내 정보보호정책은 국내에서 적용되는 13개 법령을 토대로 수립하고 정기적으로 정보보호정책 및 정책 시행문서의 타당성 검토 및 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발견, 정보보호 환경에 중대한 변화 등이 정보보호정책에 미치는 영향을 분석한다.

(2) 항만물류정보시스템 정보보호부서 구축

항만물류정보시스템 운영을 위한 회사 내 정보보호 담당부서에서 항만물류정보를 취급하고 관리하는 담당자의 지정 및 운영이 필요하며, 관리담당자는 항만물류정보시스템의 정보보호 사용권한 및 관련 업무를 총괄 관리할 수 있도록 명문화해야 된다. 항만물류정보시스템을 운영하기 위해서 요구되는 조직은 <Table 3>과 같이 구성되는 것이 필요하다.

<Table 3> Responsibilities of Each Roles

Roles	Responsibilities
Senior Manager (Wardens/heads, Vice Wardens/vice Heads)	- Ultimate Responsibility for Performance of the Agency - Developing Features Required for Task Completion, and Guaranteeing Effective Application of Required Resources - Supporting and Implementing Effective Risk Management Programs - Evaluating Results of Risk Evaluation Activities and Combining Them into Decision-Making Processes
Information Officers, Executives (CIO)	- Responsible for Port Logistics System Plans, Budget, and Results Involving Information Security Elements of the Agency - Decision-Making is based on Effective Risk Management Programs
Information Officers, Executives (CISO)	- Overall Responsibilities for Port Logistics ISMS Implementation (Including Responsibilities for Risk Management and Security Programs of the Agency) - Leads the Introduction of Methodology to Recognize, Evaluate, and Minimize Threats to Port Logistics Systems - Supporting Senior Manager for Ensuring Continuity of Activities
Security Review Committee	- Composed of Senior Manager, Heads of Work System Offices within a Range, Port Logistics Information Security Officers - Leads Port Logistics ISMS Implementation through Decision-Making
Security Officers	- Performance and Adjustment of Detailed Port Logistics ISMS Implementation Activities - Settling Party Strife during Port Logistics ISMS Implementation and Supporting Port Logistics Information Officers and Work System Officers during the Implementation Process
Work System Office Heads	- Responsible for Work Operation and Decision-Making for Purchasing Port Logistics System Required for Work - Responsibilities and Authority to Perform Decision-Making of Trade-Offs, and to Provide Resources and Support for Deciding and Obtaining the Security Level of Port Logistics Systems During Risk Management Processes
Work (System) Officers	- Owners of Port Logistics Systems and Information - Establish Appropriate Controls for their Responsible Port Logistics Systems and Data

회사 내 조직은 회사 내 여건에 따라 달라질 수 있으나, 표 3과 같이 총 7개 직급을 중심으로 회사 내 규모, 항만물류정보시스템 운영 현황 등에 따라 유동적으로 조직을 구성하고 각 직급에 대한 책임성을 명확히 하여 운영한다.

(3) 외부자 보안 구축

항만물류산업에서 취급되는 화물은 중간운송업체 등의 제3자 운송업체를 통해서 운반되는 경우가 많기 때문에 관련 운송 업무를 수행하기 위해서는 외부업체도 항만물류 정보에 접근할 수 있는 권한 설정 및 관련 보안업무 등을 정의하고 관련 기업체에서도 체계적인 정보보호를 수행해야 한다. 또한 회사 내 직원뿐만 아니라 외부인에 대한 정보 접근 및 관리 등을 수행할 수 있는 모니터링도 지속적으로 실시한다.

(4) 항만물류정보자산 분류

항만물류정보자산 분류는 회사 내에서 운영되는 항만물류정보시스템을 운영하는데 요구되는 하드웨어시스템(무인 트랜스퍼크레인 등)과 소프트웨어시스템(무인자동화 운영 시스템 등)을 분야별로 목록하여 관리해야 한다. 그 이유는 항만컨테이너터미널은 컨테이너크레인 및 장치장크레인 등의 대규모 중장비와 연계하여 운영되고 있으며, 자동화 항만컨테이너터미널 구축에 따라 다양한 자동화 장비 등도 관련 자산의 목록화를 통해 체계적인 관리한다.

(5) 항만물류정보시스템 정보보호 교육 실시

항만물류정보시스템 정보보호 교육프로그램을 지속적으로 개발하여 실시해야 한다. 항만물류산업은 제3차 산업인 서비스분야에 해당되지만, 자동화컨테이너터미널 등 IT와 정보통신 등과 연계된 통합시스템을 기반으로 운영되기 때문에 하드웨어시스템과 소프트웨어시스템 운영을 동시에 고려한 정보보호 교육프로그램이 요구되기 때문이다. 이를 위해서 항만컨테이너터미널 운영에 맞는 정보보호 교육 등의 개발 및 운영을 수행하고 일정기간별로 내부 직원 및 외부자를 대상으로 교육을 실시한다.

(6) 인적보안

인적보안은 항만물류정보시스템의 정보보호에 관한 책임의 명확성으로 항만물류정보시스템을 운영하는 담당자의 인적 정보보호 및 정보보호 권한의 오남용 등의 고의적인 행위를 줄일 수 있는 접근권한 등을 부여하다. 또한 인사 이동시 관련 권한의 반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립한다.

(7) 물리적 보안 강화

항만물류정보시스템은 선박 입출항, 화물 반출입 등의 다양한 업무를 수행함으로써 발생되는 방대한 데이터를 처리하기 위해서 데이터센터를 운영하고 있다. 회사 내 데이터센터는 물리적인 공격의 대상이 되기 때문에 엄격한 출입통제를 실시여 일반인이 쉽게 출입할 수 없도록 운영되어야 한다. 물리적 보안 강화를 위해서 출입자 출입통제시스템, 출입자 감시통제 및 지능형전력망 시스템·통신망·기기의 물리적 보호 장치를 설치하여 운영한다.

(8) 항만물류정보시스템 개별보안 확대 실시

항만물류정보시스템의 정보보호관리체계 구축 시 사용자 인증에 필요한 사용자 중요 정보의 입·출력 과정에서 정보무결성, 기밀성이 요구될 경우 법적 요구사항을 고려해야 하며, 항만물류정보시스템에는 보안로그 기능 강화로 사용자 인증, 권한 변경, 중요정보 이용 및 유출 등에 관한 내역을 보관한다. 항만물류정보시스템에서 발생될 수 해킹 등의 대내외적 공격을 사전에 진단할 수 있는 시스템을 개발하며, 개발된 진단시스템은 항만물류정보시스템이 운영될 수 있는 Windows, UNIX, PC, DBMS(Oracle, MS-SQL)에서 발생될 수 있는 취약점을 상시 진단하고 결과를 실시간 제공함으로써 항만물류정보시스템에서 발생될 수 있는 취약점 제공을 통한 개별 보안성을 높인다.

(9) 암호통제

항만물류정보시스템 관리 및 운영에 사용되는 정보보호를 위하여 암호화 대상, 암호 복잡도, 열쇠관리, 암호사용에 대한 회사 내 정책 수립 및 이행을 하며, 회사 내 중요정보는 암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 필요 시 복구방안을 마련한다.

(10) 접근통제

항만물류정보시스템을 운영하는 통제실에서는 외부인의 접근 통제, 사용자 등록 및 해지절차를 수립하고 업무 필요성에 따라 사용자 접근 권한을 최소한으로 부여한다. 카드키를 통한 사용자 인증뿐만 아니라 사용자 인증 부분에서는 항만물류정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하고. 필요한 경우 법적요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용해야 한다.

(11) 운영보안

항만물류정보시스템의 운영에서 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다. 항만물류정보시스템에 관한 새로운 정보시스템 도입 또는 개선 시 필수 보안요구사항을 포함한 인수기준을 수립하고 인수 전 기준 적합성을 검토해야 한다. 또한 항만물류정보시스템 저장매체는 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제한다.

(12) 침해사고 관리

항만컨테이너터미널 운영시스템이 외부로부터 침해사고 발생에 대비한 절차 및 체계를 구축한다. 외부 침해사고에 따른 대응 및 복구 실시를 실시하고, 침해사고 분석 및 공유 부분에서는 침해사고가 처리되고 종결된 후 이에 대한 분석을 수행하고 그 결과를 보고사후 하도록 한다.

(13) 항만물류정보시스템 재해복구

외부침해사고로 인한 항만물류정보시스템의 장애 발생 시 비상 시 복구조직, 비상연락체계, 복구절차 등 항만물류정보시스템 재해복구 체계를 구축하고 항만물류정보시스템 서비스 및 시스템 복구목표시간, 복구시점을 정의하고 적절한 복구 전략 및 대책을 수립·이행해야 한다.

Ⅴ. 결 론

우리나라는 전체 수출입 물동량의 98%를 해상운송이 담당하고 있고, 해상운송과 내륙운송의 결절점인 항만물류산업은 국제교역기능과 배후지의 경제발전을 위한 기지로서의 역할을 수행하고 있다. 수출중심국가인 우리나라에서 항만물류산업은 국가의 경제발전에 중요한 역할을 담당하고 있으나, 아직까지 항만물류산업의 정보보호 강화를 위한 노력이 매우 부족한 상황이다. 이에 본 연구는 항만물류산업의 정보보호 강화를 위한 기초연구로써 항만물류분야의 특성을 고려한 정보보호관리체계 구축 및 개선 방안을 제시하였다. 정보보호관리체계는 기업 업무 속에서 요구되는 주요 정보자산의 보호를 위해서 경영관리 체계 중의 하나로 정보자산의 보호에 관련된 정책 및 대책 수립·관리·운영하는 종합적인 체계이다. 현재 금융 산업 등을 중심으로 지속적으로 정보보호관리체계가 적용되고 있으나 현재 항만물류분야의 적용이 부족한 상황으로서 항만물류분야에서 사용되고 있는 항만물류정보시스템인 Port-MIS와 연계한 정보보호관리체계 구축단계를 5단계로 제시하였다. 또한 제시된 5단계를 통해 항만물류분야에서 정보보호관리체계를 도입하기 위해 필요한 방안을 13개로 구별하여 세부방안을 정리하여 제시하였다. 본 연구에서 제시한 구축방안 단계 및 제시된 방안을 통해서 정보보호관리체계를 구축한다면 보다 효율적인 항만물류정보를 대내외적으로 보호할 수 있는 기반이 될 것이다. 또한 정보보호관리체계 구축 및 인증을 희

망하고 있는 항만물류관련 기업체에 필요한 지침이 될 것으로 판단된다. 항만물류분야의 정보보호는 일반 기업체뿐만 아니라 국가적 차원에서 지속적인 관심과 투자가 필요한 상황으로 본 연구에서 제시한 방안을 정부차원에서 적극적인 홍보를 통한 항만물류분야의 기업체에 지속적으로 보급될 수 있는 노력이 필요하다. 본 연구는 정보보호관리체계를 기반으로 시스템적 정보보호기반을 중심으로 제시하였으나, 시스템적 정보보호분야와 물리적 정보보호분야를 연계한 통합운영시스템에 필요한 정보보호관리체계 적용과 적용에 따른 개선 효과 등의 실질적 결과 등의 제시가 향후 추가적으로 수행되어야 할 것이다.

References

Cho, Gyu-Sung(2015). Operating Plans in Grain Terminal for the Export of Grain, Journal of the Korea Society for Fisheries and Marine Sciences Education, 27(4), 1118~1128.

Jeong, Chul-Ki & Ahn, Seong-Jin(2012). A Study on the Improvements of Information Security Management System for Educational Institution, Proceeding of Korean Association Of Computer Education, 16(2), 1~4.

Jung, Chang-Hwa · Lee, Joon-Taik & Chung, Dong-Keun(2011). A Study on the Security Management System Model for the Information Security of the Aviation infrastructure, The Journal of Society for e-Business Studies, 16(4), 87~96.

Kang, Jae-Young(2013). A Study on the Systematized and unified Plan of Port Logistics Security Management System, Journal of Law and Politics Research, 13(2), 389~436.

Kim, Jeong-Deok · Jang, Hang-Bae & Ryu, Seong-Ryeol(2006). A Study of Information Security Management System for Small and Medium Enterprises, 28(2), 267~294.

Kim, Ki-Chul & Kim, Seung-Joo(2012). Evaluation Criteria for Korean Smart Grid based on K-ISMS, Journal of the Korea Institute of Information Security & Cryptology, 22(6), 1375~1391.

KLNet(2013). Strategies going into other Countries of Port Operation Information System.

Ko, Hyoung-Suk(2016). A Study on the Expansion of the Informations Protection Certification Systems, Journal of Law and Politics Research, 16(2), 411~441.

Korea Institute of Science Technology Evaluation and Planning(2007). Technology Analysis for development of Logistics Industry.

Korea Maritime Institute(2009). A Study of Development on the Port Logistics Security Industry.

Lee, Jun-Hwa · Cho, Hee-Jun · Park, Seong-Gap & Kang, Yun-Cheol(2013). Improvement of Information Security Management System on Medical Sector, Journal of the Korea Institute of Information Security & Cryptology, 23(4), 34~40.

Min, Dae-Ki(2012). A Study on the Awareness of the Logistics Security and the Improvement Plan, Chung-Ang University Master Thesis.

Won, Jong-Hyuk · Lim, Wook-Bin & Park, You-Jin (2015). A Study on Methods to Encourage the Implementation of Integrated Security Control Systems, Journal of Information Technology and Architecture, 12(4), 535~552.

● Received : 27 March, 2017
● Revised : 25 April, 2017
● Accepted : 09 May, 2017