한국항해항만학회지 제33권 제10호, pp. 735~742, 2009 (ISSN-1598-5725)
*Journal of Navigation and Port Research*

# 주요 컨테이너 터미널의 정보보호 수준 평가에 관한 연구

이 홍 걸†

† 경남대학교 e-비즈니스학부 교수

# A Study on the Evaluation of the Information Security Level in Major Container Terminals

*Hong-Girl Lee†*

† *Divison of e-Business, Kyungnam University, Masan 631-701, Korea*

**요 약** : 항만은 화물들의 정보를 토대로 거의 모든 계획과 운영이 이루어진다. 따라서, 항만에 있어 이러한 정보의 관리와 보호 문제는 매우 중요하고 근본적인 문제에 해당된다. 그러나, 이러한 중요성에도 불구하고 항만에 있어 정보보호와 관련한 연구는 매우 부족한 실정이다. 본 연구는 이러한 점에 주목하여 우리나라 주요 컨테이너 터미널의 정보보호 수준을 분석하는 것을 연구의 목적으로 하였다. 주요 컨테이너 터미널 4개사를 분석한 결과, 우리나라 컨테이너 터미널의 전반적인 정보보호 수준은 71.7%로 나타났으며, 대상 터미널 중, 3개사는 비슷한 수준과 양상을 보인 반면, 나머지 1개사는 수준 차를 보이고 있는 것으로 분석되었다. 한편, 정보보호에 있어 우리나라 컨테이너 터미널의 가장 취약한 부분은 관리적 보안인 것으로 분석되었다. 따라서, 관리적 보안의 수준을 높이기 위한 전략수립이 필요할 것으로 판단되며, 특히 정보보호를 지원하는 조직의 전문성 확보가 가장 중요한 관건인 것으로 사료된다.

**핵심용어** : 정보보호, 관리적 보안, 물리적 보안, 시스템 보안, 정보보호 지수

**Abstract** : *Information security is an essential factor that enables terminal to be operated. However, despite of this importance of information security, there has hardly been any research related to this topic. And moreover, current level of information security performance in container terminals has not been analyzed so far. The objective of this study is to evaluate current level of information security in container terminals. Through survey from the four leading container terminal operators in Korea, The results firstly showed that average of information security level of major container terminals was 71.7%. And from the results of data analysis, it revealed that the weak point of information security in Korean container terminals was security management, and in detail, lack of expertise of support group.*

**Key words** : *Information Security, Security Management, Physical Security, System Security, Information Security Index*

## 1. 서 론

오늘날 항만은 일반기업 못지않게 첨단의 정보기술에 의해 운영되고 있다. 특히, 항만은 유입되는 화물과 관련 정보를 통해 모든 것이 이루어지는 곳으로서, 항만을 거치는 모든 화물들은 필연적으로 정보를 가지고 있으며, 이러한 정보들을 통해 터미널의 거의 모든 계획과 운영이 이루어진다. 따라서, 항만은 정보에 대한 의존도가 매우 높은 곳으로서, 정보가 단절되거나 외부로 유출되면, 컨테이너 터미널의 거의 모든 기능이 마비된다고 해도 과언이 아니다(이, 2007). 그러나, 이러한 중요성에도 불구하고 최근까지 항만과 관련한 정보보호에 대한 연구는 매우 부족한 것이 현실이다.

한편, 이러한 문제에 착안하여 터미널 정보보호에 관한 연구(이, 2007)가 수행된 바 있다. 그러나, 이 연구의 경우 터미널의 정보보호 수준을 평가하기 위한 기준 수립에 관한 연구로서, 컨테이너 터미널의 실질적인 정보보호 수준 분석은 이루어지지 않았다. 따라서, 여전히 우리나라 컨테이너 터미널의 정보보호 수준에 대한 실태조차 파악되지 않고 있어, 이러한 부분에 대한 본격적인 실증연구가 필요한 실정이다.

본 연구는 이러한 선행연구에 대한 후속연구의 차원에서 우리나라 주요 컨테이너 터미널의 정보보호 수준을 분석하는 것을 연구의 목적으로 한다. 구체적으로는 본 연구에서 앞서 수행한 선행연구에서 제시된 평가기준과 평가 항목간 상대적 가중치를 토대로 우리나라 메이저급 컨테이너 터미널 4곳을 대상으로 실증적으로 정보보호 수준을 측정하여 정보보호 지수를 제시하고자 한다. 이를 통해, 터미널별 정보보호 실태와 우리나라 컨테이너 터미널의 전반적인 정보보호 수준과 취약점 등을 분석하고 몇 가지 시사점을 제안하고자 한다. 덧붙여, 본 연구에서는 선행연구에서 제안한 정보보호 수준 산출의 방법론적 측면을 보완한다. 즉, 선행연구에서 고려하지 못했던 평가영역간 상호중복성을 기존연구(류 외, 2008)의 적용방식을 이용하여 엄밀한 정보보호 수준 측정이 가능하도록 개선시켜, 이를 바탕으

† 교신저자 : 이홍걸(정회원), hglee@kyungnam.ac.kr 055)249-2420

로 컨테이너 터미널의 정보보호 수준을 분석하고자 한다.

## 2. 이론적 배경

### 2.1. 정보화와 정보보호의 기본개념

일반적으로 정보보호는 기업의 정보화 정책의 일환으로 관리되고 있다. 즉, 정보보호는 기업 정보화의 하위개념에 해당되나, 최근에는 정보보호의 중요성이 높아짐에 따라 정보보호를 독립적인 영역으로 취급하는 경향이 커지고 있다.

정보화에 대한 개념은 변화과정에 따라 정보의 산업화에 주안점을 두는 관점(Machlup, 1962; Porart, 1997)과 기술발전에 의한 사회전반의 보편적인 현상으로서 정보화를 보는 관점(Toffler, 1990), 통신중심 시각으로서 정보유통에 중점을 둔 관점(Masuda, 1980) 등이 존재한다.

한편, 정보화가 진행되어 가는 단계를 일반적으로 “정보화 성숙단계”라는 용어로 정의하고 있는데, 정보화 성숙단계란 기업조직에서 컴퓨터 도입과 관련해 전자적 자료처리(EDP: Electronic Date Processing)가 도입, 확산, 공식화, 그리고 성숙단계 등의 과정으로 성숙되어 간다는 4단계 모형에 의해서 최초로 진행 되었다. Nolan(1979)은 이를 확장하여 데이터베이스 기술 발달에 기초하여 도입, 전개, 통제, 통합, 데이터 관리, 성숙의 6단계 모형을 제시하였으며, 국내에서는 기업정보화센터(2000)에서 이를 수정하여 기업 정보화 5단계 모형을 개발하였다. 이 모형에서 정보화 성숙단계는 초기 단계인 기능 정보화단계에서 업무정보화, 기업내정보화, 기업간 정보화 최종단계인 지식정보화 단계로 구분되었다. 여기서, 정보보호는 기업내 정보화와 기업간 정보화의 하위개념에 속한다고 볼 수 있다. 특히, 정보화 단계가 성숙될수록 정보보호에 대한 중요성이 강조되고 있는데, 그 이유는 정보화가 기업간 정보화로 확대됨으로 인해, 자사의 중요 정보의 유출가능성이 그만큼 증가하기 때문이라 할 수 있다. 아울러, 정보화의 마지막단계인 지식정보화단계에서도 정보보호가 강조되고 있는 것은 기업의 정보가 기업의 지식자산으로서 발전됨에 따라, 단순히 기업내 정보를 보호하는 차원에서 기업의 자산을 보호하는 차원으로 인식이 급속히 전환되었기 때문이라 볼 수 있다.

일반적으로 정보보호라 함은 정보의 정확성을 보장하고(무결성), 정보이용과 서비스의 연속성을 유지하고(가용성), 보호되어야 하는 정보의 유출(기밀성)을 막는 것을 의미한다(한・이, 2005). 따라서, 정보보호의 가장 기본적인 목적은 무결성, 기밀성, 가용성이라 할 수 있으며, 이를 위한 구체적인 내용은 크게 관리적 차원의 정보보호와 물리적 시설을 중심으로 한 물리적 보안, 정보기술적 차원의 시스템 보안으로 구분할 수 있다(이, 2007).

### 2.2. 정보보호 평가

정보보호 수준을 평가하기 위한 연구는 개인보다 전문기관을 중심으로 주로 진행되어 왔다. 국외의 경우, 미국방성 컴퓨터의 보안성 평가를 위해 세계최초로 제안된 TCSEC(Trusted Computer Security Evaluation Criteria)(The arm of National Security Agency, 1985)와 영국에서 제안된 BS7799(BSI, 1999) 등의 연구가 대표적이라 할 수 있다. 국내 연구의 경우, 정보보호진흥원을 중심으로 정보보호 평가가 주로 수행되고 있다. 정보보호 평가와 관련한 기존 연구들을 정리하면 다음 Table 1과 같다.

Table 1 Previous research

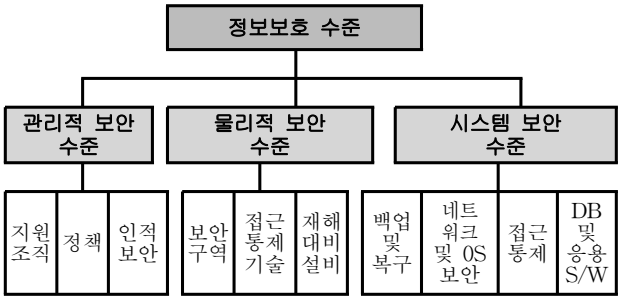
| 구분 | 내용 |
|---|---|
| TCSEC (1985) | ・미국에서 개발된 세계최초의 평가기준<br>・미국방성 컴퓨터 시스템의 보안성을 평가하기위해 개발<br>・기밀성을 중심으로 한 평가체계 |
| ITSEC (1991) | ・유럽국가들이 보안성 기준을 통합하기 위해 개발한 최초의 국제기준<br>・단일 기준으로 모든 정보보호 제품을 평가 |
| CC (1999) | ・국제 공통 평가기준(ISO5408) |
| BS7799 (1999) | ・정보보안을 유지하고 구현하는 관리자를 위한 지침<br>・평가대상이 IT보안에 집중되어 있어, 조직 전반에 관한 평가 곤란 |
| 정보보호 수준지표 (2000) | ・정보보호 투자정보 정보보호 제도 및 운영 등을 위한 지표<br>・사단법인 기업정보화지원센터에서 제공 |
| 정보화 지표 (2004) | ・한국전산원 개발<br>・정보설비, 정보이용, 정보투자지표를 기준으로 세부항목제시 |
| 정 외 (2004) | ・정보보호 기획수준, 환경수준, 지원수준, 기술수준 4가지 상위계층과 10가지 세부항목으로 지표 구성 |

출처 : 정 외(2004)의 연구를 토대로 재구성

한편, 정보보호 평가와 관련한 다수의 평가기준이 제안되었으나, 아직까지 몇 가지 문제점을 보이고 있다. 첫째, 평가기관의 성격에 따라 적용대상을 달리하고 있다는 점이다. 미국방성을 중심으로 발행된 평가기준은 주로 국가적 차원의 보안을 대상으로 하고 있어, 기업을 대상으로 한 정보보호와 다른 측면이 있다. 둘째, 평가의 내용이 조직전반보다는 컴퓨터 시스템을 대상으로 하고 있는 경우가 많다. 이러한 연구는 전사적 차원의 정보보호보다는 주로 시스템보안에 한정되어 있다. 셋째, 국내에서 주로 이루어지고 있는 정보보호진흥원의 평가는 국내기업이나 공공기관을 위주로 거시적 차원의 분석결과만 제시하고 있어, 개별기업의 구체적인 실태 파악이 곤란하고, 수립된 평가기준 역시 매우 일반적이어서 기업과 기관의 성격에 따른 차별적인 적용이 필요하다. 게다가, 본 연구의 대상인 항만과 같은 경우는 주요 평가대상이 되지 못하고 있다.

### 2.3. 평가기준의 도입

본 연구에 앞서 수행된 선행연구에서는 3가지 평가영역과 그에 따른 10가지 평가항목에 37가지 세부 측정지표로 구성된 정보보호 수준 측정을 위한 평가기준을 제안하였다. 선행연구의 평가기준은 Fig. 1과 같다.




출처 : 이홍걸(2007)

Fig. 1 Evaluation criteria of the information security

덧붙여, 선행연구에서 수립한 측정지표와 그에 따른 구성개념의 이론적 근거를 재정리한 것은 Table 2와 같다.

Table 2 Detail index for measurement

| 세부 항목 | 지표내용 | 관련문헌 |
|---|---|---|
| 지원 조직 | · 정보보호 책임자(CIO,CSO 등) 유무 | 김・나(2000), Barnard(1998), Rossouw(1998), 정 외(2004), 기업정보화센터(2004) |
| | · 보안 및 지원 조직체 운영 수준 | |
| | · 보안인력의 전문성 | |
| | · 조직의 독립성 수준 | |
| | · Help Desk의 운영수준 | |
| | · 비상시 대응 수준 | |
| | · 교육/훈련 실시 수준 | |
| 정책 | · 정책/지침/표준의 구분 수준 | Barnard(1998), Rossouw(1998), BSI(1999), 이준택(2007) |
| | · 정보보안 정책 수립 여부 | |
| | · 정보보안 정책들의 문서화 수준 | |
| | · 정보보안 표준 및 지침 수립 여부 | |
| | · 정보보안 표준 및 지침의 갱신 빈도 | |
| 인적 보안 | · 정보접근 권한의 명확성 수준 | 김・나(2000), Rossouw(1998), 정 외(2004), |
| | · 비밀유지(서약서 유무 포함) 수준 | |
| | · 보안사고 책임추적성 수준 | |
| 보안 구역 | · 보안구역(혹은 제한구역)의 명확성 | 김・나(2000), Barnard(1998), Rossouw(1998), BSI(1999) |
| | · 접근권한의 이행 수준 | |
| | · 출입통제 수준 | |
| 접근 통제 기술 | · 출입통제 기술 (보안카드, CCTV, 보안센서 등) 수준 | 김・나(2000), Barnard(1998), Rossouw(1998), 한・이(2005) |
| | · 접근통제 인력 수준 | |
| | · 사후 추적성 | |
| 재해 대비 설비 | · 전원/항온, 항습 장비 수준 | Barnard(1998), Rossouw(1998),이(2007) |
| | · 화재보호 장비 | |
| | · 재해시 비상탈출 설비 | |
| 백업/ 복구 | · 백업센터의 운영수준 | 정 외(2004), 기업정보화센터(2004), Barnard(1998) |
| | · 백업 주기 | |
| | · 복구계획/절차의 명확화 | |
| 네트워크 OS 보안 | · 바이러스 대책 | 김・나(2000), Barnard(1998), 정 외(2004), 한・이(2005) |
| | · 개인 PC 보안 수준 (보안 관련 S/W사용수준, 계정 관리수준) | |
| | · 해킹차단 기술 수준 | |
| | · 방화벽 수준 (네트워크 수준/어플리케이션 수준) | |
| 접근 통제 | · 인증 및 암호관리 수준 | Rossouw(1998), BSI(1999), 정 외(2004), 한・이(2005) |
| | · 보안 등급의 명확성 | |
| | · 접근 통제 방법 (임의적/강제적, 역할기반 통제) | |
| DB 및 응용 S/W | · 무결성 보장 수준 | 정 외(2004), 한・이(2005), 기업정보화센터(2004), BSI(1999) |
| | · 추론 방지 및 접근방지 수준 | |
| | · 파일의 접근 권한의 명확성 | |

본 연구에서는 이러한 선행연구의 후속연구로서 기 제안된 평가기준을 토대로 주요 터미널의 정보보호 수준을 분석하고자 한다.

## 3. 정보보호지수 산출체계의 수립

### 3.1. 기존 정보보호지수 산출방법의 개선

본 연구에서는 정보보호수준을 계량적으로 판단하기 용이하게 하기위해, 지수체계를 도입하고자 한다. 한편, 선행연구에서 제시한 지수산출방법은 Satty(1980)의 AHP법에 기초하여 각각의 평가영역과 평가항목 사이의 상대적 가중치를 적용한 방식이다. 그러나, 이러한 방법은 각 항목의 상호독립성을 전제로 하고 있어, 실제로 존재하거나 존재할 수 있는 평가영역간의 상호중복성을 고려하지 못하는 한계점을 가지고 있다(류 외, 2008).

따라서, 본 연구에서는 이러한 산출방법상의 문제를 개선시켜, 보다 엄밀한 평가가 가능하도록 기존의 산출방법에 퍼지평가기법을 도입하고자 한다. 본 연구에서 도입하는 방법은 Tsukamoto(1982)가 제안한 방법으로서, 적용방식은 류 외(2008)의 연구를 참고하였으며, 구체적인 적용절차는 지면관계상 생략하고자 한다.

결과적으로 퍼지평가기법을 도입한다는 것은 상기의 기존연구에서 제시한 이른바 상호작용계수 λ를 구하는 문제를 의미한다. 따라서, 상호중복성이 반영된 가중치가 수립되면, 아래와 같이 선행연구(이, 2007)의 지수산출방법을 이용하여 기존보다 엄밀한 정보보호 지수를 산출할 수 있다.

$$\sum_{i=1}^{n} W_i = 1 \quad (\text{평가영역 } i\text{의 가중치}) \tag{1}$$

$$\sum_{j=1}^{n} W_{ij} = 1 \quad (\text{평가영역 } i\text{에 있어, 평가항목 } j\text{의 가중치})$$

또한, 평가영역( $i$)의 평가항목에 대한 점수를 $S_{ij}$로 한다면,

$S_i = \sum_{j=1}^{n} W_{ij} S_{ij}$ (평가영역 $i$의 점수) 가 되며,

$Nor(S_i) = S_i \times \frac{100}{i\text{영역의만점}}$ 의 과정을 통해, 실제 점수 $S_i$ 를 정규화한다.

따라서, 최종적인 정보보호 지수 $S$는,

$S = \sum_{i=1}^{n} W_i Nor(S_i)$ 로 된다.

### 3.2. 상호중복성을 고려한 가중치 산출을 위한 실증조사

전 절에서 언급한 바와 같이 선행연구에서 수립한 상대적 가중치에는 평가영역간 상호중복성이 고려되지 않았으므로, 제안한 방법론의 수순에 의거하여, 새롭게 평가영역의 상대적 가중치를 수립하고자 한다.

이를 위해서는 상호중복성 계수를 구하기 위한 실증적 차원

의 추가조사가 필요하다. 특히, 본 연구의 특성상, 항만관련의 실무자 및 연구자의 경우에도 정보보호와 관련한 지식과 연구의 경험이 없으면 조사에 참여시키기 곤란하므로, 대학 및 연구기관에서 물류정보를 연구하고 있는 연구자들을 중심으로 설문조사의 범위를 우선적으로 한정시켰다.

본 조사는 2008년 9월에 최종적인 설문시트가 완성되었으며, 본격적으로 설문이 배포되어 조사가 이루어진 기간은 10월1일부터 11월10일까지로 대략 40일간 수행되었다. 추가조사에 참여한 총 인원은 연구자 20명이었으며, 여기에 선행연구에서 수행된 상대적 가중치 수립을 위한 조사대상을 합치면, Table 3과 같이 총 51명의 설문조사 데이터가 활용되었다.

Table 3 The Collection of questionnaire

| | | | |
|---|---|---|---|
| 직책 | 정보전산팀 | 25명 | 49.0% |
| | 일반관리팀 | 6명 | 11.8% |
| | 연구자 | 20명 | 39.2% |
| 근속연수 | 5년미만 | 10명 | 32.3% |
| | 5~10년 | 18명 | 58.1% |
| | 10년이상 | 3명 | 9.7% |

※ 본 연구에서 추가로 조사된 인원은 연구자 20명이며, 나머지 조사대상은 선행연구(이, 2007)에서 수행된 내용임

### 3.3. 평가가중치 산출

본 연구에서는 평가영역간 상호중복성이 고려된 최종적인 정보보호 지수 산출체계를 수립하기 위해, 우선 본 연구에 앞서 수행된 선행연구(이, 2007)의 평가영역 및 평가항목간의 상대적 가중치를 활용한다. 선행연구에서 제시한 상대적 가중치는 각각 Table 4, Table 5와 같다.

Table 4 Previous weight values of factors

| 구분 | 관리적 보안 | 물리적 보안 | 시스템 보안 | 가중치 | CR |
|---|---|---|---|---|---|
| 관리적 보안 | 1.000 | 0.333 | 2.000 | **0.252** | 0.046 |
| 물리적 보안 | 3.000 | 1.000 | 3.000 | **0.589** | |
| 시스템 보안 | 0.500 | 0.333 | 1.000 | **0.159** | |

상기의 평가영역간 상대적 가중치를 수정하기 위해, 상호중복성과 관련하여 추가로 수집된 데이터를 토대로 평가영역간 상호작용계수를 산출한 결과는 Table 6과 같다. 수립한 상호작용계수 $\lambda$를 이용하여, 상호중복성을 고려한 최종적인 평가영역 가중치를 구한 결과는 Table 7과 같다.

Table 5 Weight values of sub factors

| 평가영역 | 평가항목 | 가중치 | CR |
|---|---|---|---|
| 관리적 보안 | 지원조직 | **0.268** | 0.007 |
| | 정책 | **0.537** | |
| | 인적보안 | **0.195** | |
| 물리적 보안 | 보안구역 | **0.288** | 0.045 |
| | 접근통제기술 | **0.448** | |
| | 재해대비설비 | **0.263** | |
| 시스템 보안 | 백업 및 복구 | **0.125** | 0.024 |
| | 네트워크 OS | **0.263** | |
| | 접근통제 | **0.517** | |
| | DB 및 응용 | **0.095** | |

즉, 평가영역의 가중치는, 선행연구에서 산출한 가중치에 평가영역간 상호중복성을 고려하여 최종적으로 관리적 보안수준 0.244, 물리적 보안수준 0.597, 시스템 보안수준 0.159로 수정되었다. 덧붙여, 하위계층에 해당하는 세부 평가항목의 가중치는 선행연구에서 구한 Table 5의 결과 값을 그대로 활용하면 된다.

Table 6 Interaction weight values of factors

| 구분(영역) | 상호작용 |
|---|---|
| 관리적 보안수준 | -0.350 |
| 물리적 보안수준 | -0.300 |
| 시스템 보안수준 | -0.316 |
| 상호작용계수 $\lambda$ = -0.319 | |

Table 7 The final weight values of factors

| 구분(영역) | 선행연구의 상대적 가중치 | 상호작용을 고려한 최종적인 가중치 |
|---|---|---|
| 관리적 보안수준 | 0.252 | **0.244** |
| 물리적 보안수준 | 0.589 | **0.597** |
| 시스템 보안수준 | 0.167 | **0.159** |

## 4. 정보보호 수준 분석

### 4.1 분석개요

분석에 참여한 터미널 운영사는 우리나라에서 활동하고 있는 대표적인 운영사 4곳으로서, 허치슨, PECT, 동부, PNC를 대상으로 하였다. 한편, 본 연구내용의 특성상 4곳의 관계자 모두 연구결과가 실명으로 공표되는 것을 꺼려하여, 익명을 요구하였다. 따라서, 구체적인 분석결과는 익명으로 제시하고자 한다. 조사는 2008년 11월 17일부터 12월 5일 사이에 실시되었다.

조사는 사전에 각 터미널의 정보팀장과 정보팀 소속관계자와 연락하여, 시간 계획을 세워 해당 일에 서면질의 방식으로 인터뷰를 실시하였다.

인터뷰는 본 연구에서 제안한 정보보호 평가기준을 토대로 질문시트를 작성하여 그 것을 토대로 진행하였다. 질문서는 “매우 부족(혹은 매우 나쁨)”을 1점으로 하고 “매우 충분(혹은 매우 좋음)”을 5점으로 표현한 5점 척도 방식으로 구성되었다. 인터뷰는 참여자가 각 질문항목을 충분히 이해한 후에 이루어졌으며, 각 항목마다 참여자의 답변을 뒷받침할 수 있는 근거를 제시하거나, 그 이유를 실례로서 청취하는 방식으로 확인조사가 동시에 이루어 졌다.

3.1절에서 제안한 방법론에 의거하여 터미널 4개사의 정보보호 수준을 산출한 결과를 정리하면 Table 8과 같다. 분석결과로부터, 대상 터미널 중에서 가장 높은 정보보호 수준을 보유한 터미널은 A 터미널(78%)로 나타났으나, C 터미널(75.6%)과 큰 격차를 보이고 있지 않다. D 터미널의 경우, 상위 2개사에 비해 뒤쳐져 있으나, 평가영역 전반에 걸쳐 거의 비슷한 수준분포를 보이고 있는 것으로 분석되었다. 또한, 분석결과로부터 주목할

만한 것은 B 터미널의 경우 다른 터미널과 격차가 다소 나고 있다는 점이다. 특히 모든 평가영역에서 60점대에 머물러 있어 정보보안을 위한 대책수립이 가장 시급한 터미널인 것으로 나타났다.

한편, 우리나라 주요 컨테이너 터미널의 정보보호 수준의 평균은 71.7%로 나타났다. 절대적인 기준치가 없어 수준의 높고 낮음을 명확히 언급하기 곤란하지만, 우리나라 주요 컨테이너 터미널의 정보보호 수준이 전반적으로 우려할 만한 것은 아니나, 터미널 운영 수준을 높이기 위해서는 정보보호 수준 향상을 위해 계속적인 투자와 관리가 필요한 상황인 것으로 판단된다.

### 4.2 평가영역별 비교분석

컨테이너 터미널 4개사의 관리적 보안 수준을 비교한 결과는 Fig. 2와 같다. 비교 결과로부터, 터미널별로 관리적 보안 수준의 격차가 발생하고 있는 것을 알 수 있다. 컨테이너 터미널 4개사의 관리적 보안 수준 평균은 64.9%로 분석되어, 전체 정보보호 수준 평균 71.7%에 미치지 못하고 있음을 알 수 있다. 즉, 관리적 보안이 전체 정보보호 평가 영역 중에서 대표적인 마이너스 요인으로 작용하고 있어, 컨테이너 터미널의 대표적인 취약점이라 할 수 있다.

Fig. 3은 관리적 보안의 세부항목을 비교분석한 결과이다. 비교결과로부터, 각 평가항목별로 높은 수준을 보이고 있는 터미널이 각기 다름을 알 수 있으나, D 터미널의 경우 평가항목 모두에서 대부분 낮은 수준을 보이고 있다. 따라서, D 터미널의 경우 관리적 보안 전체에 대한 개선책 마련이 필요한 상황이다.

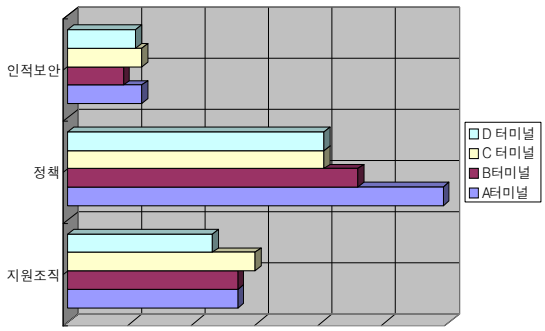



Fig. 3 Comparative analysis of the detail factors in security management

한편, B 터미널의 경우, 다른 항목에 비해 인적보안 수준이 상대적으로 낮은 것으로 나타났다. 특히, 인적보안의 수준은 조직문화와 조직내부의 분위기, 관례에 의해 좌우되는 측면이 강하다. 게다가, 인적보안이 통상 시스템 보안 보다 더 심각한 보안문제를 초래할 가능성이 높으므로 B 터미널은 이 부분에 대한 전사적 차원의 쇄신책을 마련할 필요가 있을 것으로 사료된다.

4개 터미널의 물리적 보안 수준을 비교하면 Fig. 4와 같다. 4개 터미널의 물리적 보안 수준 평균은 72.9%로 산출되었으며, 4개 터미널 중 가장 물리적 보안 수준이 높은 터미널은 C 터미널이며, 반면에 가장 낮은 터미널은 B 터미널인 것으로 분석되었다.

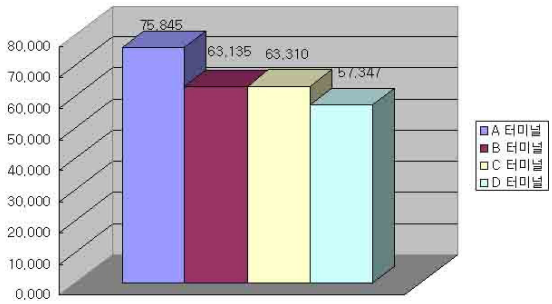



Fig. 2 Security management levels of major terminals

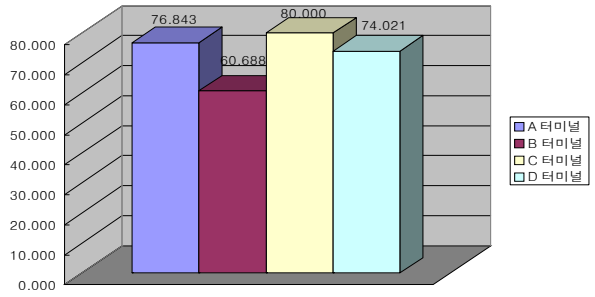



Fig. 4 Physical security levels of major terminals

Table 8 Information security index of four major terminals

| 평가 영역 | 세부 평가항목 | A터미널 | | B터미널 | | C터미널 | | D터미널 | |
|---|---|---|---|---|---|---|---|---|---|
| | | 항목점수 | 평가영역 점수 | 항목점수 | 평가영역 점수 | 항목점수 | 평가영역 점수 | 항목점수 | 평가영역 점수 |
| 관리적 보안 | 지원조직 | 5.360 | 18.506 | 5.360 | 15.405 | 5.896 | 15.448 | 4.556 | 13.993 |
| | 정책 | 11.822 | | 9.136 | | 8.061 | | 8.061 | |
| | 인적보안 | 2.335 | | 1.752 | | 2.335 | | 2.141 | |
| 물리적 보안 | 보안구역 | 3.172 | 45.875 | 2.884 | 36.231 | 3.460 | 47.760 | 3.460 | 44.191 |
| | 접근통제기술 | 4.933 | | 3.587 | | 5.381 | | 4.484 | |
| | 재해대비설비 | 3.422 | | 2.632 | | 3.159 | | 3.159 | |
| 시스템 보안 | 백업/복구 | 1.871 | 13.607 | 1.372 | 10.820 | 1.497 | 12.207 | 1.622 | 12.493 |
| | 네트워크 및 OS 보안 | 5.267 | | 3.423 | | 3.687 | | 3.950 | |
| | 접근통제 | 5.691 | | 5.174 | | 6.209 | | 6.209 | |
| | DB및 응용S/W 보안 | 1.134 | | 1.134 | | 1.134 | | 1.040 | |
| 정보보호 지수 | | 77.988 | | 62.456 | | 75.414 | | 70.676 | |

특히, Fig. 4로부터 3개사의 물리적 보안수준은 대략 70%중반에서 80점 정도로 큰 격차를 보이고 있지 않지만, B 터미널의 경우 이들 터미널과 격차를 보이고 있는 것을 알 수 있다. 게다가, 앞서 분석한 Table 8의 결과를 토대로 판단해 보면, B 터미널의 정보보호 부문 중 가장 취약한 부분이 바로 물리적 보안 부분임을 알 수 있다.

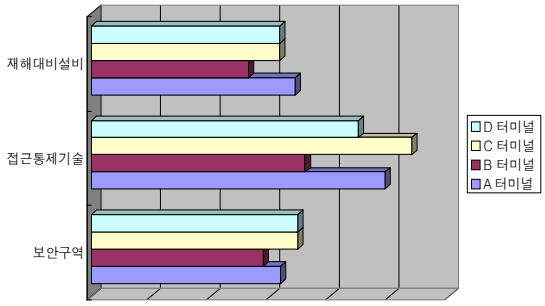



Fig. 5 Camparative analysis of the detail factors in physical security

Fig. 5는 물리적 보안의 세부항목을 비교한 결과이다. C 터미널의 경우 재해대비 설비를 제외한 모든 항목에서 가장 높은 보안수준을 나타내고 있는 반면, B 터미널은 모든 세부 항목에서 상당한 격차를 보이며, 가장 낮은 수준에 머물러 있음을 알 수 있다. 특히, 다른 터미널과 가장 큰 격차를 보이고 있는 항목은 접근통제기술로 나타났다. 따라서, B 터미널이 다른 터미널의 수준과 어깨를 나란히 하기 위해서는 특히 접근통제기술 부문의 개선책이 우선적으로 고려되어야 할 것이다.

시스템 보안 수준을 비교한 결과는 Fig. 6과 같다. 그림으로부터 가장 시스템 보안 수준이 높은 것으로 나타난 터미널은 A 터미널이며, 반면에 B 터미널이 시스템 보안 수준이 가장 낮은 것을 알 수 있다. 또한, C와 D 터미널의 경우 대략 비슷한 수준을 보이고 있는 것으로 파악되었다.

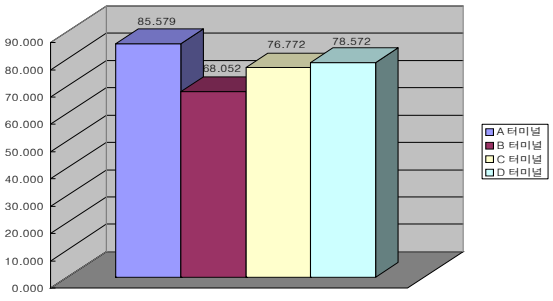



Fig. 6 System security levels of major terminals

특히, 시스템 보안 수준의 전체 평균은 77.2%로써, 3가지 평가영역 중에서 가장 높은 수준을 보이고 있는 것으로 나타났다. 따라서, 시스템 보안은 정보보호 수준의 강점요인으로 작용하고 있음을 알 수 있다. 시스템 보안의 세부 평가항목을 비교한 결과는 Fig. 7과 같다.

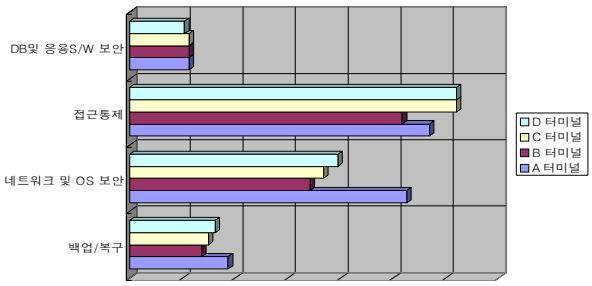



Fig. 7 Camparative analysis of the detail factors in system security

평가항목별 마다 수준이 고르게 분포되어 있어, 시스템 보안에 있어 각 터미널에서 주안점을 두고 있는 부문이 다르다는 것을 짐작할 수 있다. 그러나, 여전히 B 터미널의 경우 DB 및 응용S/W 보안 부문을 제외한 모든 항목에서 가장 낮은 수준을 보이고 있고, 시스템 보안의 전체 수준도 다른 터미널과 격차를 보이고 있는 것으로 나타났다.

한편, 네트워크 및 OS보안의 경우 터미널 마다 서로 다른 수준차를 보이고 있는 것으로 나타났다. 특히, A 터미널과 나머지 터미널 사이의 격차가 비교적 많이 나타나고 있는데, 확인조사 결과 네트워크 보안 중에서 해킹과 관련한 지표가 가장 많은 격차를 보이고 있는 것으로 파악되었다. 즉, A 터미널에 비해 나머지 터미널의 경우, 해킹 방지기술을 도입하고는 있으나, 그 중요성과 전문성은 A 터미널에 비해 상대적으로 떨어지고 있는 것으로 파악되었다. 특히, 보안사고가 발생하기 전에는 그 중요성에 대해 그다지 인지하지 못하고 있으나, 정보보호에 있어 가장 기술적인 전문성을 요하는 영역이 해킹과 관련한 영역이므로, 이 부분에 대한 전문성 확보가 필요할 것으로 판단된다.

### 4.3 분석결과의 정리 및 시사점

이상의 과정을 토대로 우리나라 주요 컨테이너 터미널의 정보보호 수준과 관련한 분석결과와 그에 따른 몇 가지 시사점을 정리하면 다음과 같다.

첫째, 우리나라 주요 컨테이너 터미널의 정보보호 수준은 평균 71.7% 수준인 것으로 나타났다. 즉, 전반적으로 우려할 만한 수준은 아니나, 수준향상을 위한 계속적인 투자와 관리가 필요할 것으로 사료된다.

둘째, 4개사의 컨테이너 터미널을 분석한 결과, 3개 터미널(A, C, D 터미널)은 비슷한 수준의 양상을 보이고 있으나, 1개 터미널(B 터미널)이 나머지 3개 터미널과 수준 차를 보이고 있는 것으로 나타났다. 특히, B 터미널의 경우 거의 모든 측면에서 다른 대상 터미널에 비해 낮은 수준을 보이고 있어, 정보보호 수준 향상을 위한 전략 수립이 절실한 상황으로 판단된다.

셋째, 정보보호에 있어, 우리나라 주요 컨테이너 터미널의 가장 취약한 부분은 관리적 보안이며, 반면에 강점은 시스템 보안

인 것으로 분석되었다. 특히, 관리적 보안의 세부 항목 중에서 무엇보다 지원조직의 전문성 확보가 가장 큰 관건인 것으로 파악되었다. 따라서, 각 터미널별로 정보보호의 전문성 확보를 위한 방안을 자체적으로 마련하여 관리적 보안의 취약점을 보완해 갈 필요가 있다.

넷째, B 터미널의 경우 정보보호 수준이 가장 낮은 것으로 분석되었으며, 모든 영역이 다른 터미널에 비해 뒤떨어진 것으로 나타났다. 따라서, B 터미널이 정보보호 수준을 향상시키기 위해서는 정보보호 전 영역에 걸친 전략수립이 필요할 것으로 사료된다. 특히, 그 중에서도 물리적 보안 수준이 다른 터미널과 가장 많은 격차를 보이고 있는데, 이를 향상시키기 위한 자체적인 대책이 필요하며, 다른 컨테이너 터미널을 벤치마킹하여 비슷한 수준으로 시급히 물리적 보안 수준을 끌어올릴 필요가 있다.

## 5. 결 론

본 연구는 지금까지 연구가 매우 미흡하였던 컨테이너 터미널의 정보보호 문제에 주목하여, 우리나라 주요 터미널 4개사의 정보보호 수준을 실증적으로 측정하여 전반적인 정보보호 수준과 그에 따른 취약점 등을 도출하였다. 또한, 선행연구의 지수 산출 방법상의 문제를 개선시켜 보다 엄밀한 계산이 가능하도록 기존의 평가영역 가중치를 수정하였다.

본 연구에서 제시한 정보보호 수준과 취약점 등은 항만물류 분야에 있어 지금까지 도출된 바 없는 새로운 영역의 지표로서 향후 실무적 차원이나 학술적 차원에서 컨테이너 터미널의 정보보호 수준을 고려하는 문제에 있어 참고지표로 이용될 수 있을 것으로 기대된다.

한편, 본 연구는 아직까지 한계점을 가지고 있다. 첫째, 정보보호 수준이라는 운영사의 입장에서 다소 민감한 문제를 다루므로 인해, 참여대상을 확보하는데 매우 곤란한 측면이 있어, 결국 4개사에 국한하여 분석이 진행되었다. 따라서, 본 연구의 결과를 우리나라 컨테이너 터미널 전체로 일반화하기에는 아직까지 조심스러운 측면이 있다. 둘째, 정보보호 수준을 측정하기 위한 방식에는 설문을 통한 인식조사와 실제 실험 및 검수를 통한 조사가 측정내용의 성격에 따라 병행되어 수행되어야 하나, 본 연구에서는 상기에서 언급한 동일한 이유로 인해 실제 실험과 직접측정을 수행할 수 없었다. 따라서, 조사에 참여한 각 터미널의 정보팀장의 의견과 그에 따른 근거에 의존하여 측정된 값으로서, 향후 이러한 부분에 대한 보완이 필요할 것으로 사료된다.

셋째, 본 연구에서는 선행연구에서 수립한 평가기준을 그대로 활용하고 있는데, 선행연구의 경우 연구내용에 잘 부합하는 표본을 확보하는데 문제가 있어 결과적으로 통계적 신뢰성을 확보하지 못했다. 따라서, 본 연구에서도 이러한 한계점을 여전히 가지고 있어, 평가기준의 신뢰성 확보를 위한 기초연구가 계속적으로 이루어져야 할 것이다. 끝으로, 본 연구는 컨테이너 터미널의 정보보호 수준을 분석하는데 주안점을 두고 있어, 터미널의 정보보안 미비로 인한 문제를 해결하기 위한 구체적인 대안 제시가 부족한 측면이 있다. 따라서, 이를 위한 면밀한 추적조사와 이를 바탕으로 한 개선방안에 관한 연구가 과제로 남아있다.

## 후 기

본 논문은 인하대학교 정석물류통상연구원의 지원에 의하여 연구되었음(INHA-JRI-2008)

## 참 고 문 헌

[1] 기업정보화지원센터(2004), 기업정보화수준평가 결과보고서, 기업정보화지원센터.

[2] 김기윤, 나관식(2000), “취약성 평가에 의한 정보보호 지표의 계량화 : 정보자산 가중치법”, 한국정보보호학회지, 제10권 제1호, pp.51-62.

[3] 류형근, 이홍걸, 이철영(2007), “항만의 정보화 수준 제고를 위한 통합평가지수 개발에 관한 탐색적 연구”, 한국항해항만학회지, 제31권, 제6호, pp. 491-496.

[4] 류형근, 이홍걸, 이철영(2008), “주요 컨테이너 터미널의 정보화 수준 분석에 관한 연구”, 한국항해항만학회지, 제32권 제3호, pp.199-205.

[5] 이준택(2007), 정보보호학개론, 생능출판사.

[6] 이철영, 이석태(1993), “상호연관성을 지닌 계층구조형 문제의 평가 알고리즘”, 한국항만학회지, 제7권 제1호, pp.5-125.

[7] 이홍걸(2007), “컨테이너 터미널의 정보보호 수준 제고를 위한 통합평가지수 개발에 관한 연구”, 해운물류연구, 제54호, pp.99-118.

[8] 정희조, 김진영, 임춘성(2004), “기업의 정보보호수준 및 성숙도 진단을 위한 정보보호수준 통합평가시스템 개발에 관한 연구”, 정보보호학회지, 제14권 제4호, 한국정보보호학회, pp.37-44.

[9] 한국전산원 (1994), 국가정보화종합지수 모델개발 연구.

[10] 한명묵, 이철수(2005), 『정보보호개론』, 정익사.

[11] Barnard, L.(1998), "The Evaluation and Certification of Information Security against BS7799," Information Management & Computer Security, Vol.6, No.2, pp.72-77.

[12] BSI(1999), BS7799, BSI.

[13] Commission of the European Communities(1991), "Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria".

[14] ISO/IEC15408(1999), The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC).

[15] Rossouw, S.(1998), "Information Security Management(3) : the Code of Practice for Information Security Management,"

Information Management & Computer Security, Vol.6, No.5, pp.224-225.

[16] Satty, T.(1997), The Analytic Hierarchy Process, Mcgraw-Hill Book Co.

[17] The Arm of National Security Agency(1985), TCSEC (Trusted Computer Security Evaluation Criteria), NCSC.

[18] Tsukamoto, Y.(1982), "Transformation Form Probability Measures to Fuzzy", Journal of Japan Automatic Measurement and Control, Vol.19, No. 3, pp.269-270.

원고접수일 : 2009년 9월 29일
심사완료일 : 2009년 11월 30일
원고채택일 : 2009년 12월 1일