

국가 물류보안 체제 확립방안 연구(I)

2006. 12.

최재선 · 목진용 · 황진회 · 고현정



한국해양수산개발원
KOREA MARITIME INSTITUTE

□ 보고서 집필 내역

◆ 연구책임자

- 최 재 선 : 제1장, 제3장, 제5장 ~ 제7장

◆ 연구진

- 목 진 용 : 제2장 ~ 제5장
- 황 진 회 : 제3장 ~ 제5장
- 고 현 정 : 제2장 ~ 제4장

◆ 외부 집필진

- Ru Yihong (중국북경교통대학교) : 제4장
- 이카와 테츠오 (IMOS) : 제4장
- 유 광 의 (한국항공대학교) : 제4장
- 한 범 수 (이비테크) : 제6장

□ 산·학·연·정 연구자문위원

- ◆ 황 경 철 (대한항공)
- ◆ 김 길 섭 (한국무역협회)
- ◆ 담 당 관 (국가정보원)
- ◆ 권 순 태 (해양수산부)
- ◆ 허 삼 녕 (해양수산부)
- ◆ 오 동 연 (해양수산부)
- ◆ 김 영 무 (한국선주협회)
- ◆ 손 을 호 (관 세 청)
- ◆ 최 원 백 (투디엔디)
- ◆ 주 형 태 (아이토스)
- ◆ 양 희 준 (한국생산성본부)
- ◆ 김 인 수 (이비테크)

머 리 말

물류보안이 새로운 국제 현안으로 떠오르고 있다. 2001년 미국에서 일어난 9·11 항공기 테러 이후 미국을 비롯해 국제사회에서 여러 가지 보안조치를 마련하고 있기 때문이다. 특히 테러 피해국은 미국은 그 동안 해운보안법과 컨테이너 보안 협정 등 여러 가지 물류보안조치를 마련하여 시행하고 있는 가운데, 2006년 10월에는 다시 항만보안법을 제정해 자국뿐만 아니라 글로벌 보안 제도를 더욱 강화하고 있다.

국제기구는 미국의 보안제도를 글로벌 기준으로 채택, 세계적인 시행을 주도하고 있다. 국제해사기구가 미국의 해운보안법을 모태로 국제선박 및 항만시설 보안에 관한 규칙(ISPS Code)을 제정해 2004년 7월부터 시행에 들어간 데 이어 세계세관기구도 미국의 CSI와 C-TPAT를 통합한 ‘물류보안과 무역 간소화에 관한 국제기준’을 채택, 100여 개국이 시행하기로 합의하였다.

이와 같이 물류보안제도가 글로벌 메가 트렌드로 정착되고 있어 수출입 화물의 보안을 확보하고, 위험성을 확인하는 것이 시급한 과제로 등장하고 있다. 미국은 앞으로 수입되는 모든 컨테이너 화물에 대해서는 100% 사전 검색을 추진한다는 방침으로 있어 우리나라 수출 기업의 부담이 더욱 커질 전망이다. 특히 최근 항만보안법을 제정한 미국이 외국항만에 국제컨테이너 검색 네트워크(ICSN) 구축에 착수함에 따라 일정한 보안활동이 이루어지지 않은 화물에 대해서는 강도 높은 검사가 예상되는 등 무역장벽으로 작용할 가능성도 커지고 있다.

물류보안제도는 물류 전 구간의 보안을 확보해 궁극적으로 테러를 차단하는 효과뿐만 아니라 화물 운송의 가시성을 높이고, 컨테이너 화물의 신속한 처리로 물류비를 절감할 수 있다는 이점이 있다. 그러나 물류보안을 확보하는데 따른 비용 증가와 교역구조를 왜곡한다는 부정적인 의견도 있는 것이 사실이다.

그러나 이 같은 찬반양론 속에서도 싱가포르와 홍콩 등은 물류보안 고도화

를 항만 마케팅 전략으로 활용하고 있어 관심을 끌고 있다. 컨테이너 터미널에서 수출·환적 화물의 방사성 물질 포함여부 등을 점검하고, 화물의 안전성 보장을 서비스로 인식, 인근 항만과의 차별화를 통해 경쟁력 및 화물 유치에 적극 활용하고 있다.

물류보안이 강화됨에 따라 이에 관련된 사업도 각광을 받고 있다. 물류보안 산업이 일자리 창출 및 새로운 비즈니스 영역으로 부상하고 있기 때문이다. 우리 원이 추정한 바에 따르면, 컨테이너 보안장비 부착 의무화 등으로 물류보안 시장이 2010년에는 연간 50억 달러에 달할 것으로 추정되고 있다. 이와 같이 물류보안 산업이 새로운 성장 동력으로 부상됨에 따라 시장을 선점하기 위해 록히드 마틴, GE 등 글로벌 기업 사이의 경쟁도 치열한 실정이다.

이 연구보고서는 9·11 테러 이후 미국과 주요국에서 이루어지고 있는 물류보안제도를 한데 모으고, 앞으로 우리나라 정부 및 기업의 대응 전략을 수립하기 위해 작성된 첫 번째 산물이다. 우리 연구원은 물류보안의 중요성과 시급성을 판단, 이 연구사업을 기획과제로 선정해 2006년과 2007년 2개년도 사업으로 수행하고 있다. 2006년도 1차년도 사업은 각국의 물류보안제도와 우리나라의 관련 제도와 문제점을 파악하는데 중점을 두었다. 이 같은 연구결과를 토대로 2007년에는 우리나라 물류 보안 전략을 수립할 계획으로 있다.

연구보고서를 작성하는 과정에서 해양수산부뿐만 아니라 관련 분야의 많은 전문가들이 자문과 도움을 주셨다. 물류보안이 아직 학문적으로 정립되지 않았고, 그 개념 또한 생소한 분야이기 때문에 전문가들의 지원이 이 연구보고서 발간이 큰 도움이 되었다. 지면을 빌어 다시 한번 감사의 말씀을 드린다. 앞으로 이 연구보고서가 물류보안제도를 이해하고, 연구하는데 새로운 지평을 열고, 정부는 물론 기업들이 대응전략을 수립하는데 도움이 되기를 기대한다.

2006년 12월

韓國海洋水產開發院

院 長 李 正 煥

목 차

ABSTRACT	i
----------	---

요 약	v
-----	---

제1장 서 론	1
---------	---

1. 연구의 배경과 목적	1
1) 연구의 배경과 필요성 / 1	
2) 연구의 목적 / 4	
2. 선행연구 내용의 분석	7
3. 연구의 주요 내용과 수행방법	8
1) 연구의 주요내용 / 8	
2) 연구 방법 / 10	

제2장 운송 수단별 테러와 보안 취약요인	13
------------------------	----

1. 세계 정치 환경 변화와 테러	13
1) 동시다발적 테러의 발생 / 13	
2) 국제 사회의 테러 대책 / 14	
2. 물류 공급망에서의 보안위협	16
1) 보안위협에 대한 현안 / 16	
2) 공급망에서의 테러 공격 및 방법 / 19	
3) 운송시스템에서의 보안 위험 / 22	
3. 물류보안 취약 요인 분석	25

- 1) 물류 공급망의 주요 활동 주체 / 25
- 2) 물류 공급망의 취약점 / 27

제3장 국제기구의 물류보안제도인 시사점 ————— 31

1. 국제해사기구(IMO)	31
1) 솔라스(SOLAS)협약 개정 / 31	
2) ISPS Code / 35	
3) 해상불법행위억지협약 / 39	
4) 시사점 / 51	
2. 국제관세기구(WCO)	52
1) WCO의 프레임워크 / 53	
2) WCO의 프레임워크 표준안 / 56	
3) 시사점 / 72	
3. 국제표준화기구(ISO)	72
1) ISO의 물류보안 인증 / 72	
2) ISO의 보안관리 시스템 / 74	
3) 시사점 / 84	
4. 국제민간항공기구(ICAO)	84
1) ICAO 동경협약 / 85	
2) 항공기의 불법납치 억제를 위한 협약 / 86	
3) 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약 / 88	
4) 국제 민간항공기 취항공항에서 불법폭력행위 억제 의정서 / 88	
5) 탐지목적의 플라스틱 폭발물 표시에 관한 협약 / 89	
6) 국제민간항공협약 부속서17 항공보안 규정 / 90	
7) ICAO 항공보안지침서 문서 8973/6 / 91	
8) 시사점 / 91	

제4장 주요국의 물류보안 정책과 시사점 94

1. 미국의 물류보안제도 94
 - 1) 국토안보부(DHS) 신설 / 94
 - 2) 컨테이너 보안협정 시행 / 97
 - 3) 화물정보 선적 24시간 전 신고제도 / 100
 - 4) 민·관 협력 반테러 보안제도 / 101
 - 5) 해운보안법 제정·시행 / 102
 - 6) 연안경비대 등의 운수 근로자 신분 통제 / 107
 - 7) 항만보안법 제정·시행 / 109
 - 8) 시사점 / 112
2. EU의 물류보안제도 113
 - 1) 현행 EU 물류보안 여건 / 113
 - 2) EU 물류보안 여건개선 노력 / 117
 - 3) EU 공급망 보안강화 규정 / 120
 - 4) 시사점 / 129
3. 일본의 물류보안제도 130
 - 1) 부문별 물류보안제도 / 130
 - 2) 해운업계의 보안대책과 과제 / 133
 - 3) 향후 일본의 물류보안 대책 / 139
 - 4) 시사점 / 140
4. 중국의 물류보안 제도 141
 - 1) 부문별 물류보안제도 / 141
 - 2) 물류보안 시설·장비 개발 / 143
 - 3) 중국의 물류보안 과제 / 145
 - 4) 중국과 외국의 물류보안 협력 / 147
 - 5) 시사점 / 152

제5장 우리나라 물류보안제도 시행 현황————— 154

1. 보안관련 법률과 각 부처의 업무	154
1) 국방부 / 154	
2) 국가정보원 / 156	
3) 해양수산부 / 157	
2. 해운·항만 부문 보안 제도	159
1) 관련 규정 / 159	
2) 항만경비보안 주체 및 운영방식 / 161	
3) ISPS Code의 발효와 국내 대응조치 / 164	
3. 항공·공항 부문 보안제도	174
1) 항공보안의 역사와 개념 / 175	
2) 국가의 항공보안 책임과 공항의 보안활동 표준 / 179	
3) 우리나라의 항공보안제도 / 192	
4. 철도부문 보안제도	194
1) 철도 대테러 방호지침 / 195	
2) 철도 역사의 보안 시스템 / 197	

제6장 우리나라 물류보안제도 문제점과 정책방향————— 201

1. 우리나라 물류보안제도의 문제점	201
1) 물류보안제도 수용상의 문제점 / 201	
2) 운송 모드별 문제점 / 207	
2. 물류보안에 대한 관련기관의 의견	225
1) 한국 선주협회 / 225	
2) 한국 무역협회 / 226	
3) 다른 기관 의견 / 227	
3. 물류보안제도 정책방향	228

- 1) 물류보안 강화에 따른 대책 수립 / 228
- 2) 통합 물류보안 시스템 구축 / 230
- 3) 물류보안 기술 및 표준 확보 / 232
- 4) 물류보안의 고도화·비즈니스화 / 234

제7장 결론 및 정책 제언 237

- 1. 연구 결론 237
 - 1) 물류보안의 글로벌화 및 영역 확대 / 237
 - 2) 물류보안에 대한 이해 및 인식 부족 / 238
 - 3) 정부 관계 부처간 업무 조정 미흡 / 239
 - 4) 주요 무역국과의 물류보안협력 필요 / 240
 - 5) 민간 기업의 자발적 참여 방안 마련 / 241
 - 6) 물류보안시장 선점 및 지원 전략 부족 / 242
- 2. 정책 제언 244
 - 1) 우리나라 물류보안 체제의 세계화 / 244
 - 2) 물류보안의 고도화·고품격 서비스화 / 246
 - 3) 물류보안을 새로운 성장동력으로 활용 / 248

참고문헌 251

표목차

<표 1-1>	선행 연구현황 및 선행 연구와의 차별성	8
<표 1-2>	주요 연구내용	9
<표 2-1>	운송모드별 테러 공격 대상	20
<표 2-2>	테러 방법	21
<표 2-3>	보안 위험 피해 예측	24
<표 2-4>	공급망에서의 활동 주체	26
<표 2-5>	각종 물류보안제도의 특징	27
<표 3-1>	AIS 탑재시기	32
<표 3-2>	2005년 SUA 협약의 주요 내용	44
<표 3-3>	범죄협의선박에 대한 승선 · 검색 절차	49
<표 3-4>	항공테러 발생 현황	86
<표 4-1>	CSI 시행 항만 및 미 입항 물동량	98
<표 4-2>	미 관세청 24시간 규칙의 주요내용	100
<표 4-3>	미국 해운보안법의 내용	104
<표 4-4>	미국 및 국제기구의 물류 보안 제도	105
<표 4-5>	SAFE Port Act 중 국제물류 관련 주요내용	110
<표 4-6>	화주(생산지에서 화물의 선적준비와 선적관련 활동자)의 특별요건	123
<표 4-7>	운송회사의 특별요건	124
<표 4-8>	운송주선회사의 특별요건	125
<표 4-9>	창고 · 보관시설 · 육상터미널(내륙항만 포함) 운영자의 특별요건	126
<표 4-10>	위험평가	127

<표 5-1>	국가중요시설의 분류	155
<표 5-2>	부산항 경비·보안업무 책임 분장	162
<표 5-3>	ISPS Code 시행을 위한 사전 대응조치	164
<표 5-4>	협약시행을 위한 사전 추진현황	167
<표 5-5>	국가민간항공보안 프로그램의 내용	180
<표 5-6>	한국공항공사 공항보안예산 지원 내용	194
<표 5-7>	인천국제공항공사 공항보안예산 지원 내용	194
<표 5-8>	철도 대 테러 경보발령단계(요약)	196
<표 6-1>	우리나라 컨테이너 화물 검사기 설치 현황	205
<표 6-2>	전국 컨테이너항만의 화물검색기 조달현황 및 재원	206
<표 6-3>	각 지방해양수산청별 ISPS Code 적용대상 항만 현황	209
<표 6-4>	각 보안주체별 인력 현황	210
<표 6-5>	특수경비원 신임교육의 과목 및 시간	219
<표 6-6>	전술에 따른 테러 현황(1968~2005년)	221
<표 6-7>	미국 물류보안제도의 글로벌화	228
<표 6-8>	홍콩항만의 컨 물동량 및 항만 보안료 징수 현황(추정)	236

그림목차

<그림 1-1>	연구 수행 흐름도	11
<그림 3-1>	보안관리 시스템의 구성요소	74
<그림 4-1>	미 국토 안보부 조직도	96
<그림 4-2>	CSI 처리 절차	99
<그림 4-3>	운영자의 최소한의 필요조건	127
<그림 5-1>	부산항만 경비보안 지휘체계	163
<그림 5-2>	광양항 컨테이너부두의 지휘 · 감독 체계	163
<그림 5-3>	선박보안 인증절차	165
<그림 5-4>	항만보안 인증절차	169
<그림 5-5>	철도역사 내부전경	197
<그림 5-6>	역사 출입구 감시 시스템	198
<그림 5-7>	역사 감시 모니터 장비	199
<그림 5-8>	출입구 지문인식 시스템	199
<그림 5-9>	카드키 출입통제시스템	199
<그림 5-10>	역사 실내외의 각종 카메라	200
<그림 6-1>	항공화물 보안시스템에서 보안검색시점	216
<그림 6-2>	물류보안제도 적용 범위	230

ABSTRACT

After the World Trade Center attacks in New York by terrorist groups on September 11, 2001, security assurance across international trading system is becoming a critical factor for international business managers and governments. While the initial concern of crisis management was on vulnerability to the air transportation system, the attention moved to security in the maritime sector and then regarding inland transport. Accordingly, the international organizations and United States have actively developed a number of initiatives focusing on global security issues.

Certain international organizations such as International Maritime Organization (IMO), World Customs Organization (WCO), and International Organization for Standardization (ISO) have supported enhancing regulatory coverage of safety and security within the world trading system. In the maritime sector, IMO implemented the new security plans set out in International Ship and Port Facility Security (ISPS) Code, which contained detailed security related requirements for governments, port authorities, and shipping companies together with a series of guidelines to meet these requirements. ISPS is one of a number of amendments to the 1974 Safety of Life at Sea Convention (SOLAS). WCO also developed a regime in order to enhance the security and facilitation of international trade, which was the WCO Framework of Standards to Secure and Facilitate Global Trade. And ISO developed the Publicly Available Specification (PAS

28000) for a security management standard to improve the security of supply chains.

In addition, the United States has actively promoted a series of voluntary trade programs in order to enhance security of trade into U.S. seaports. The two principle voluntary programs are the Container Security Initiative (CSI) and the Customs-Trade Partnership against Terrorism (C-TPAT). CSI was implemented by entering into bilateral agreements which allowed both nations to send inspectors to each other's ports. The inspectors had the authority to inspect containers being shipped by sea. C-TPAT sought to develop cooperative relationships among companies in the global supply chain and the U.S. authorities.

In order to cope with these circumstances of security assurance, the Korea Maritime Institute initiated a two-year project (2006~2007) for establishing Korea's supply chain security system. Security issues became all the more pressing since effective and efficient systems of transportation with security assurance are critical to domestic and international business. Along with trade liberalization, the adoption of international standards, advanced telecommunications, and the capacity to securely transport goods are critical factors in globalized and interdependent economies. Thus, effective and efficient systems of transportation with security assurance are critical to optimizing transport and transaction costs and global competitiveness generally. Based on this, the first of the two year projects investigated current supply chain security issues of various nations and international organizations and then identified Korea's security related challenges to be concerned. Based on these findings, next year's project will provide a national master plan for supply chain security systems including detailed action plans.

The contents of this year's study consist of seven major chapters. Chapter 1 provides an overview of the objectives of the study and research methodologies. Chapter 2 addresses the threat of international terrorism on various transport modes and their vulnerability. Chapter 3 discusses the security issues developed by IMO, WCO, ISO, and ICAO and their implications. Chapter 4 also discusses the security issues from various nations such as the United States, EU countries, Japan, and China and their implications. Chapter 5 addresses Korea's current status of supply chain security systems. Chapter 6 investigates Korea's supply chain security problems and provides a discussion of policy implications as well as strategies for assuring a national supply chain security. Finally, Chapter 6 provides conclusions and political proposals for the Korean government.

As a result, the conclusions of this year's study can be summarized in the following way: Firstly, security assurance moves into a whole-of-supply chain issue from a framework of independent transportation security regime. Second, although the pressure on security issues is gradually strengthened, shipping lines and companies in Korea regards them as burdensome, so that they are still passive to follow the international security regimes. Third, the Korean government is also ill-informed about supply-chain security issues. Additionally, each ministry is accustomed to take charge of its own business so that there is no an administration to handle the national supply chain security from an integrated point of view. Fourth, developing close relationships and partnerships with other countries is an important element to ensure efficient implementation of supply chain security. However, the Korea seems to lack concern about cooperation even with major economic trading partners. Fifth, the national supply chain security program cannot be successfully implemented only by the public sector attention as the role of

private sector participation is very important. So, there should be an institutional system in Korea in order to draw attention of the private sector. Finally, the security-related industry is emerging as national economic growth power and its market size is expected to increase up to \$4~5 billion. However, only few companies have an interest in this market and the government is not at all interested in it.

In addition, the following three major political suggestions in this study are made: Firstly, making the national supply chain security standards global is urgent. For this, there can be three possible alternatives, which are – to set up a committee for national supply chain security; to develop highly advanced port security systems in major ports; and to create integrated supply chain security systems. Secondly, ensuring logistics competitiveness in security is necessary by way of providing enhanced security services. For this, there can be three possible alternatives – which are to incorporate and vitalize a certificate system for supply chain security; to develop relationships and partnerships with other countries for fast customs clearance; and to adopt security certification of transshipment cargoes. Finally, developing strategies of supply chain security as national economic growth power is required. For this, there can be three possible alternatives – which are to standardize and commercialize logistics equipment and technology; to create a system for gathering and analyzing various security information and data; and to nurture the security related industries as a next-generation growth engine.

요 약

제1장 서론 : 연구의 배경과 목적

1. 물류 보안 패러다임의 변화

- 2001년 9·11 테러 이후 해운·항만 등 국제물류 전반의 보안 강화와 화물 흐름의 효율성 제고가 국제사회의 중요한 현안으로 부각되고 있음
 - － 상품의 생산지에서 최종 소비지에 이르는 물류 전 구간에서 테러가 발생하는 경우 인명과 재산 피해는 물론 국제 교역로가 차단되는 물류 왜곡현상이 일어날 수 있기 때문임
 - － 또한 선적항이나 양하 항에서 화물에 대한 안전조치를 강화하고, 컨테이너에 대한 검사비율을 높일 경우 화물의 지체 현상이 발생해 선박은 물론 화주에게도 막대한 피해를 줄 수 있음
- 이 같은 우려에도 불구하고, 물류보안제도를 시행하는 경우 테러 방지는 물론 화물운송 시간 29% 단축, 수송상의 문제 해결시간 31% 단축, 화물의 도난 37% 감소라는 긍정적인 효과도 있는 것으로 조사됐음

2. 새로운 교역 장벽으로 등장

- 최근 미국을 중심으로 도입되고 있는 물류보안제도는 눈에 보이지 않는 무역장벽으로 작용할 가능성도 매우 큰 것도 사실임
 - － 예컨대, 미국이 2002년에 도입한 반테러 민-관 파트너십 제도(C-TPAT)의 경우 보안기준을 제대로 준수하게 되면, 우선 통관이 보장되나 그렇지 않으면 입항 거부와 같은 불이익을 받을 수 있기 때문임
 - － 또한 물류보안제도 시행과 관련하여 컨테이너 화물 검색기나 보안장

- 치(CSD), 스마트 컨테이너, 전자 태그(RFID), 화물 추적 장치 등의 개발과 국제표준을 둘러싸고 관련업체간 기술 선점 경쟁도 치열해지고 있음
- 싱가포르와 홍콩 등은 자국의 물류보안기준을 높여 환적 화물 유치 등 물류 경쟁력을 강화하는 전략을 구사하는 등 기존의 국가와는 다른 방향에서 보안제도를 활용하고 있음

3. 정부 · 민간부분의 관심 부족

- 우리나라의 경우 정부 부처 간에 통합적으로 물류보안을 관할하는 정책이 없는 것이 가장 큰 문제점으로 지적되고 있음
- 건교부가 항공보안 및 안전에 관한 법률을, 해양수산부가 국제선박 및 항만시설의 보안에 관한 규정을 시행하고 있으나 전 운송 구간을 통합적인 차원에서 규율하는 제도가 없음
- 또한 지난해부터 동북아 최첨단 지능형 U Port 사업을 시행하고 있으나 이 같은 시스템은 국제적으로 요구되고 있는 물류보안표준과 차이가 있어 향후 시스템 통합과 정보교환 등에서 문제가 발생할 소지도 있음
- 특히 우리나라의 경우 일부 부처와 대기업을 제외하고는 국제적으로 강화되고 있는 물류보안제도에 대한 이해가 크게 부족하고, 정부와 민간 부분의 협력체제도 구축되어 있지 않음

4. 향후의 국가 물류보안기본계획 수립

- 이 같은 현실을 배경으로 이 연구에서는 크게 다음과 같은 두 가지 목적을 설정하고 2년 동안 연구를 수행하고 있음
- 첫째, 현재 강화되고 있는 물류보안제도의 진원지인 미국의 제도가 어떤 것이 있고, 앞으로 어떻게 변할 것인지 파악하는 한편, 이 같은 제도가 어떤 과정을 거쳐 글로벌 보안 기준으로 정착되는지 집중 분석할 예정임
- 둘째, 우리나라 물류보안제도의 문제점이 무엇인지 파악하고, 국제적인 흐름에 맞춰 앞으로 기존 제도를 어떻게 고쳐야 하는지 검토한 다음(제1차년도), 국가 물류보안 기본계획(제2차년도)을 수립하는 데 있음

※ 특히 이 과제는 해양수산부 등이 추진하고 있는 ‘물류보안 종합대책’ 수립과 연계하여 연구를 진행하고 있음

〈요약 표-1〉 국가 물류보안 체제 확립방안 연구 내용

연구년도	주요 연구 내용
2006년(1차년도) 연구	주요국의 물류 보안 제도 조사 및 분석, 시사점 분석, 정책 제언
2007년(2차년도) 연구	국가 물류보안체제 구축 방안 및 세부전략 작성 - 국가 물류보안 계획 수립 및 물류보안 기술 및 장비 개발 대응방안 등 포함

제2장 운송 수단별 테러와 보안 취약요인

- 컨테이너 화물의 국제적 이동을 고려할 때, 화물의 생산지에서 최종 소비자에 이르는 모든 구간이 테러로 피해를 입을 가능성이 있음
 - 특히 최근 들어 자유무역협정(FTA) 등으로 국가간 교역이 확산되고, 생산 공장 이전 등으로 컨테이너 화물의 운송 거리가 길어짐에 따라 위험 또한 늘어나고 있음
 - 2004년 국제해사기구(IMO)에서 ISPS 코드를 도입함에 따라 선박 및 항만 부문에 대한 보안은 어느 정도 강화됐으나 육상 운송구간은 아직도 취약한 부문이 많은 것으로 분석됨
 - 이에 따라 미국은 항만보안법을 제정, 국제물류보안 전략계획 수립을 의무화했으며, 유럽연합과 싱가포르도 ‘통합 물류보안계획’을 수립·시행한다는 방침임
- 한편, 테러 등으로 항만 등 물류 기간시설이 파괴되거나 기능이 중단될 경우 입을 수 있는 피해액은 천문학적인 수치에 달할 것으로 추정되고 있음
 - 2002년의 부즈 앨런 해밀톤 위 게임 시나리오에 따르면, 미국 LA 항만 및 사반나 항만에서 Dirty Bomb이 발견되어 항만이 4주 동안 운영이 중단될 경우 47억 달러의 손실을 입을 것으로 산정

- 또한 이 같은 테러는 미국뿐만 아니라 아시아 지역에도 영향을 미쳐 아시아 경제성장률이 0.4% 정도 하락하고, 특히 홍콩과 싱가포르, 말레이시아의 경우 성장률이 1.1% 떨어지는 것으로 분석됐음
- ※ 테러로 수에즈 운하나 파나마 운하, 말라카 해협이 봉쇄되는 경우 국제 물류 마비 등 엄청난 파급효과 초래

〈요약 표-2〉 운송 구간별 테러 공격 대상

구분		운송 모드			
		해상	항공	철도	도로
물류 인프라	운송로	해상교통로	항공로	철로 터널 다리 교차로	도로 터널 다리 교차로
	환적 장소	항만터미널	공항터미널	화물터미널 철도정차 야드	물류터미널
시설 오염 측면	통제 시스템	해상운송 관리 시스템	항공운송 시스템	중앙 통제소 지방 통제소	도로 운송관리 시스템
	통신 시스템	통신망	통신망	신호체계	통신망
	종업원	선원 하역인력 보수인력 정보처리 인력	승무원 하역인력 보수인력 정보처리 인력	기관사 하역인력 보수인력 정보처리 인력	운전수 하역인력 보수인력 정보처리 인력
	운송수단	선박 바지	비행기	화차 차량	트럭 트레일러
운송 화물		비위험화물 폭발화물 유독물 가연화물	비위험화물 폭발화물 유독물 가연화물	비위험화물 폭발화물 유독물 가연화물	비위험화물 폭발화물 유독물 가연화물

제3장 외국의 물류보안제도 및 시사점

1. 물류보안제도 시행 현황

- 현재 시행되고 있는 물류보안제도는 미국과 국제기구를 중심으로 9·11 테러 이후 도입되고 있는 것이 대부분인데,

- 첫째, 선박과 항만 등 특정지역을 적용대상으로 하고 있는 제도와 둘째, 제품의 생산에서 소비에 이르는 모든 물류 구간을 적용대상으로 하고 있는 제도로 대별할 수 있음
 - 특정 구간을 적용대상으로 하고 있는 제도는 미국의 CSI와 24시간 규칙, 그리고 IMO의 ISPS 코드 등이 대표적이며,
 - 컨테이너 전 운송 구간을 대상으로 하고 있는 제도는 미국의 C-TPAT와 WCO의 물류보안 기본협정(국제교역의 안전과 간소화를 위한 국제기준(Framework of Standard to Secure and Facilitate Global Trade), OECD 및 유럽연합의 전 운송구간 물류보안 규칙 등이 있음
- ※ EU의 물류보안규칙은 2006년 2월에 입법예고 된 뒤 의견 수렴을 거쳐 지난 12월에 최종 확정됐음
 - 또한 싱가포르는 아시아 권 국가로서는 처음으로 2006년 안에 ‘국가물류보안계획’을 수립, 시행한다는 방침임

〈요약 표-3〉 주요국 및 국제기구의 물류 보안 제도

구분		주요 내용	도입 · 시행
미국	행정부	○ 국가보안부 설치 등 행정 조직 개편 - 연안경비대 등 통합, 인원 17만명	2003년 1월
	관세청	○ 컨테이너 보안 대책(CSI)제도 도입 - 세계 20대 항만 화물 검색 강화	2002년 1월
		○ 반테러 민-관 파트너십(C-TPAT)제도 - 제품의 공급사슬 보안관리시스템	2002년 4월
		○ 에너지부와 합동으로 대형항만 방사능 탐지 제도 시행	2005년 3월
		○ 적하목록 24시간 사전 신고제도 도입 - 관세청 규칙 개정, 모든 선사 적용	2003년 1월
	연안경비대	○ 여객선에 화물 탐지기 · 보안요원배치 - 규정 위반 선사에 입항 금지 조치	2002년 7월
		○ 교통안전청과 합동으로 운수근로자 신원조사 및 신분증 발급제도 도입 (캐나다도 동일제도 시행)	2006년 5월
		○ 해군 · 연안경비대 합정 보안지역 지정	2001년 10월
		○ 96시간 전 선박 입항 예정시간 통보제	

주요국 및 국제기구의 물류 보안 제도 (계속)

구분		주요 내용	도입 · 시행
미국	국무부	○ 선원의 미국 항만 입국 요건 강화 - 선원의 항만 비자 명부 삭제	2003년 1월
		○ 테러 가능성 선원의 선내 억류 제도 - 미국 다른 항만으로 확대 · 적용	2002년
	법무부	○ 국가 보안 출입관리제도 도입 - 미국 방문자의 지문 날인제도	항만 입국선원 우선 적용
	의 회	○ 해운 보안법 제정	시행
		○ 항만보안법 제정	2006년 10월
IMO	법 률 위원회	○ 2005년 항해안전협약(SUA) 제정 - 범죄인의 소추 및 외국 인도 가능	2005년 10월
	해 사 안 전 위원회	○ 국제 선박 및 항만 보안 규칙 제정 - 1974년 해사인명안전협약 개정	2002년 12월
	총 회	○ 해사 테러리즘 대응 결의서 채택 - 회원국의 보안제도 평가, 대응 권고	2001년 11월
WCO	총 회	○ 새로운 공급사슬 보안제도 도입 - CSI · C-TPAT 모델의 세계 규범화	2005년 7월
E U	회원국 공통	○ 물류 보안 규칙 제정 추진	2006년 2월 입법예고
민 간 부 문	허치슨, 싱가포르 PSA	○ Smart and Secure Tradelane - 민간 차원의 해사보안 프로그램	2002년 7월

2. 외국 물류보안제도 시사점

- 미국식 보안 기준의 글로벌화 확산
 - 현재 시행되고 있는 물류보안제도는 사실상 미국의 제도를 국제적으로 시행하고 있는 것과 같음
 - IMO의 ISPS 코드는 미국이 2002년에 제정한 해운보안법의 내용을 대부분 원용했으며,
 - WCO의 물류 보안 기본협정도 미국이 2002년부터 시행하고 있는 C-TPAT와 CSI 및 24시간 규칙의 기본 정신과 골격을 받아들인

것임

- 따라서 미국의 제도와 향후의 입법 동향을 정확하게 파악, 대응하는 것이 시급함

〈요약 표-4〉 미국 물류보안제도의 글로벌화

구 분	초기단계	성숙단계	최종단계
시행방법	업계의 자발적 참여 유도	법률에 의한 강제 집행	국제협약으로 세계 규범화
시행근거	양자 협약	입법 조치	다자 협약
참여기관	미국 관세청	미국 의회	국제해사기구 및 세계세관기구 등
이행수단	인센티브 제공	처벌 규정 도입	회원국의 의무
시행시기	2001~2002	2002~2004	2004년 이후

- 통합 물류보안이 새로운 현안으로 부각
 - 9·11 테러 이후 물류보안제도는 미국의 CSI와 IMO의 ISPC 코드 등에 따라 선박과 항만의 보안조치와 일부 외국항만에서 미국행 화물에 대한 컨테이너 검사가 대부분이었음
 - 그러나 이 같은 제도가 점차 정착되기 시작한 2004년 이후부터는 물류 전 구간의 보안을 강화하는 등 적용 영역이 점차 확대되고 있음
 - ※ 미국의 경우 C-TPAT를 의무화하는 방안을 추진하고 있으며, 유럽 및 WCO 등 전구간의 통합물류보안 강화조치 도입
 - 이 같은 경향은 앞으로 우리나라가 특정 구간의 보안뿐만 아니라 화물의 전 유통 구간에 대한 보안을 통합적인 시각에서 다시 검토해야 한다는 것을 시사함
- 물류보안 기술 및 표준선점 경쟁 치열
 - 물류 보안제도가 국제적으로 강화됨에 따라 이와 관련된 기술개발과 국제 표준을 둘러싸고 글로벌 대기업간 이합집산과 경쟁도 치열해지고 있음

- 이는 향후 40억~50억 달러로 추정되고 있는 컨테이너 화물 검사장비와 방사능 탐지장비, RFID와 화물추적장치 등을 포함한 이른바 ‘스마트 컨테이너’ 시장이 더욱 확대될 가능성이 있기 때문임
- 현재 국제 물류보안 장비 시장은 미국의 사비 테크놀로지를 인수한 록히드 마틴 그룹과 최근 국제컨테이너 보안 협회(ICSO)를 창설한 제너럴 일렉트릭을 중심으로 하는 그룹으로 양분되어 있음
- 우리나라의 경우 이 같은 국제적인 움직임과는 별도로 독자적인 RFID 시스템을 구축할 예정으로 있어 향후 국제 기술 표준 등을 놓고 갈등이 불가피할 가능성도 있음

제4장 우리나라 물류보안제도 및 정책방향

1. 기존의 물류보안제도

- 우리나라는 남북이 대치하고 있는 특수상황 때문에 다른 나라에 비해 국가 중요시설에 대한 보안조치는 비교적 양호한 것으로 평가되고 있음
- 통합 방위법에 따라 국가 중요시설의 소유자 또는 관리자에 대해 경비·보안책임을 지고, 통합방위사태에 대비하여 자체방호계획을 수립하도록 요구하고 있음
- ※ 그러나 통합방위법은 적의 남침 등에 대비해 시설에 대한 방호를 염두에 두고 제정한 법률이기 때문에 물류 보안 측면에서는 원용할 수 있는 규정이 많지 않은 것이 사실임
- 해운·항만 부문에서는 앞에서 언급한 통합방위법에 따른 항만보안규정 등이 우선적으로 적용되고, 2004년 7월부터는 ISPS 코드를 수용한 고시를 시행하고 있음
- ※ 해양수산부에서는 2007년 1월 시행을 목표로 가칭 ‘선박 및 항만시설 보안에 관한 법률’을 입법 예고하고, 가을 정기 국회에 처리할 계획으로 있어 이 부문에 대한 입법 조치는 매듭지어지고 있음

- 또한 항공부문도 항공안전 및 보안에 관한 법률을 시행하고 있어 적어도 법적으로는 테러 등 외부의 충격에 대처할 수 있는 시스템은 구축되어 있다고 할 수 있음
- 이 밖에도 우리나라는 컨테이너 보안 협정(CSI) 시행과 관련하여 2003년에 미국과 협정을 체결하여, 부산항에서 미국행 화물에 대한 보안검사를 실시하고 있음

2. 앞으로의 물류보안제도

- 한편, 우리나라는 최근 국제적으로 물류보안이 더욱 강화됨에 따라 항만뿐만 아니라 물류 전구간의 보안을 강화하는 여러 가지 조치를 도입하기 시작했음
- 해양수산부는 최근 국제선박 및 항만시설 보안에 관한 법률을 제정하는 것을 계기로 ‘항만 보안체제 정비 및 보안역량 강화방안’을 검토하고 있으며,
- 동북아 물류추진기획단 또한 현재 국제적으로 강화되는 물류보안 추세를 우리나라 항만 경쟁력 제고에 활용하는 방안을 추진하고 있음
- 관세청은 2005년 8월 WCO가 채택한 물류보안에 관한 Framework를 국내에서 시행하는 방안의 하나로 최근 ‘공인 파트너관리시스템(C-APM)’을 구축하고 2010년까지 시행한다는 방침임
- 이에 앞서 해양수산부는 2005년부터 항만운영 효율화 사업의 하나로 전자태그(RFID) 구축사업에 착수, 오는 2008년까지 끝낼 방침으로 있는 등 각 분야에서 다양한 물류보안사업이 추진될 예정으로 있음

3. 물류보안제도의 문제점

- 우리나라 물류보안제도가 안고 있는 문제점은 1) 국내 자체적인 문제점과 2) 국제 환경변화에 따른 문제점 두 가지로 집약할 수 있음
- 첫째, 자체적인 문제점으로는 내륙 운송부문의 경우 물류 보안을 담보

- 할 수 있는 법적 기반이 없어 도로 및 철도의 경우 테러 등 위험사태에 그대로 노출되어 있다는 점임
- 예컨대 생산 공장에 대한 보안기준이나 컨테이너 화물의 적입과정에 대한 보안통제가 전혀 이루어지고 않고 있고,
 - 컨테이너를 적재한 트럭이 항만 게이트를 통과할 때 운전기사에 대한 통제와 신분확인이 이루어지고 않고 있음
 - 또한 항공부문도 외국 항공사의 보안 검색 능력문제, 상용화주제도 도입문제, 보안경비요원의 능력과 높은 이직률, 고도화되는 테러에 대한 대체 능력 등 여러 가지 문제점이 제기되고 있음
 - 한편, 항만 부문에서는 ISPS 코드 시행으로 보안상태가 많이 개선됐으나 형식적인 대처가 대부분이라는 지적임
 - ※ 항만 감시 카메라의 경우 관세청과 항만 경비보안업체가 별도로 운영하고 있어 예산낭비가 심하고, 일부 터미널의 경우 가장 기본적인 출입자 통제조차 제대로 이루어지지 않고 있음
- 둘째, 국제 환경 변화에 따른 문제점으로는 화물 공급 사슬 전반을 통합적으로 관리하는 물류보안제도가 구축되어 있지 않다는 점임
- 미국의 C-TPAT의 경우 제품 생산에서 판매에 이르는 전 구간의 완벽한 보안 확보를 요구하고 있으며, 유럽연합이나 싱가포르 등도 이 같은 추세에 따르고 있음
 - 특히 우리나라의 경우 물류 보안 장비 및 기술개발과 투자, 협력을 소홀히 함에 따라 향후 국제 표준 경쟁에서 낙오될 가능성도 배제할 수 없음
 - 더 큰 문제는 국제적으로 물류보안제도가 강화되고 있음에도 일부 부처와 기업을 제외하고, 이 같은 움직임을 제대로 파악하지 못하고 있어
 - 물류 보안을 강화할 수 있는 민관 협력 프로그램이 부족하고, 전문가 양성이나 국제 협력 등에 전혀 관심을 기울이지 못하고 있다는 점임
 - ※ 싱가포르와 홍콩, 일본, 중국 등은 자국의 보안기준을 글로벌 기준

에 맞추는 한편, 이 같은 흐름을 적극 활용, 환적 화물 유치는 물론 궁극적으로 국제 경쟁력을 높이는 지렛대로 활용하는 전략을 추진하고 있음

4. 앞으로의 물류보안정책 방향

- 물류보안제도가 앞으로 글로벌 메가 트렌드로 정착되고 있어 이에 대한 대비책을 마련하는 것이 시급한 실정임
 - － 전문가들은 컨테이너 화물의 안전성 확보가 앞으로 상당기간 국제적인 중요 해결 과제로 대두될 전망이라는데 거의 일치하고 있음
 - － 이에 따라 세계적인 물류보안 강화 동향을 수동적으로 수용하기보다는 적극적인 활용 전략이 절실함
 - － 또한 우리나라 항만 경쟁력 확보와 물류 서비스 고도화를 위해 국가 물류보안 전략이 필요한 실정임
- 물류보안이 확산되는 초기단계에서 완벽한 보안시스템을 구축하고, 필요한 제도를 마련하는 것이 앞으로의 국제적인 물류 경쟁에서 유리한 것으로 판단되고 있음
 - － 미국 등 주요 무역국에는 우리항만을 거친 화물의 안전성을 보장, 재점검 등으로 인한 지연과 추가 비용의 발생을 방지하고,
 - － 아시아의 화주 등에게는 우리 항만을 세계로 화물을 운송하기 위한 가장 신속하고, 안전한 항만으로 인식시켜 화물 유치에 활용하는 정책이 필요함
- 또한 물류보안 산업을 육성하고, 관련 기업이 세계시장에 진출할 수 있도록 성장기반을 구축하는 것도 시급한 전략의 하나임
 - － 거대 시장으로 성장하고 있는 물류보안 산업을 선점하는 한편, 국내 일자리 창출과 기업의 이익 창출에 기여할 것이 분명하기 때문임
- 한편, 한국선주협회의 한국무역협회 등은 국제적인 추세에 따라 우리나라의 물류보안제도를 강화하는 데 대체적으로 동의하고 있음

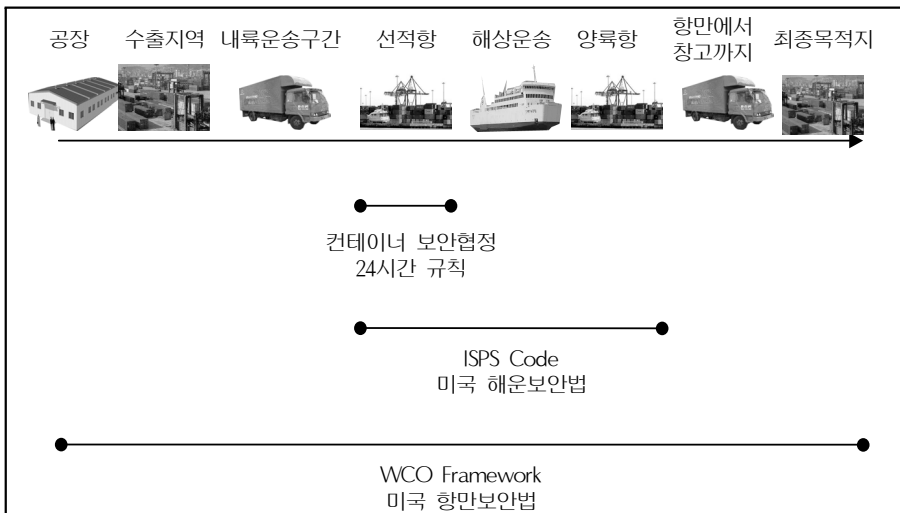
- 다만, 각 행정부처가 개별적으로 물류보안제도를 도입할 경우 이중삼중의 부담이 뒤따르고,
- 원활한 물류 흐름도 저해할 우려가 있으므로 통합적인 방향에서 이 같은 제도를 도입하는 것이 바람직하다고 주문하고 있음

제5장 정책 제언과 2차년도 연구 내용

1. 연구 결론

- 물류보안의 글로벌화 및 영역 확대
 - 물류보안제도가 초기의 항만이나 선박을 중심으로 이루어지던 단계에서 벗어나 물류 전 구간으로 확대되고 있으며, 개별 국가 위주에서 글로벌 기준으로 정착되고 있음

〈요약 그림-1〉 물류보안제도 적용 범위 및 확대 동향



- 물류보안에 대한 이해 및 인식 부족
 - 미국을 포함해 물류보안제도가 크게 강화되고 있음에도 우리나라 선사 기업들의 경우 부담요인으로 인식하고 있으며, 수동적인 자세에서 제도를 이행하고 있는 것으로 파악되었음
- 정부 관계부처간 업무 조정도 미흡
 - 우리나라 정부 또한 물류보안제도에 대한 이해가 부족하고, 각 부처의 경우 소관 업무만을 처리할 뿐 물류 전 구간을 통합적인 차원에서 처리하는 정책이 없는 실정임
 - ※ 해양수산부에서 추진하고 있는 전자태그 시스템 구축 사업의 경우 건교부와 업무 조정문제로 육상구간에 대한 리더기 설치가 지연되고 있음
- 주요 무역국과의 물류보안협력 부족
 - 물류보안업무를 효율적으로 처리하기 위해서는 다른 교역 상대국과의 긴밀한 협력이 필수적이거나 우리나라의 경우 이에 대한 대처와 협력이 거의 없는 실정이며, 그나마 피동적인 자세를 견지하고 있음
 - ※ 관세청은 2003년에 미국과 CSI 협정을 체결하고, 협력을 증진하고 있으나 컨테이너 화물 검색기는 수출화물이 아닌 수입화물 검색에 주로 사용
- 민간 기업의 자발적 참여 방안 결여
 - 물류보안은 정부의 일방적인 주도로 이루어질 수 없으며, 그 효과를 확대하기 위해서는 화주 등 민간기업은 자발적인 참여가 필요하나 물류보안에 대한 이해가 극히 낮아 민간 참여를 유도할 수 있는 제도적 장치가 거의 없음
- 물류보안시장 선점 · 지원 방안 전무
 - 물류보안산업이 차세대 성장 동력으로 부상하고 있고, 향후 시장 규모가 40~50억 달러로 커질 것으로 예상되고 있으나 우리나라 일부 기업을 제외하고는 이에 대한 참여나 준비가 전혀 없으며, 정부 또한 예외가 아님

2. 정책 건의

- 앞으로 우리나라는 다음과 같은 세 가지 틀에서 물류보안정책을 추진하는 것이 바람직한 것으로 분석됐음
- 첫째, 우리나라 물류보안 체제를 세계화하는 것이 시급한데, 그 대안으로,
 - (1) 국가 물류보안 협의체 구성·운영,
 - (2) 고성능·최첨단 항만보안 시스템 확보,
 - (3) 완벽한 통합 물류보안 시스템 구축을 제안함
- 둘째, 물류보안의 고도화·고품격 서비스화로 우리나라 항만 및 물류 경쟁력을 확보하는 것이 필요한데, 그 대안으로
 - (1) 물류보안 인증제도 도입, 활성화,
 - (2) 주요국과 화물 신속통관 협정 체결,
 - (3) 환적 화물에 대한 보안인증제 도입 등을 제안함
- 마지막으로, 물류보안을 새로운 성장 동력으로 활용하는 전략을 개발해야 하는데, 그 대안으로,
 - (1) 물류보안 장비·기술 표준화, 상용화,
 - (2) 물류보안 정보 수집·활용 조직화,
 - (3) 물류보안을 차세대 성장산업으로 육성 등을 제시하고자 함

3. 향후 연구

- 2007년 연구에서는 제1차년도 연구 내용을 토대로 국가 물류보안기본 계획 수립과 물류보안장비 개발 및 시장 선점 전략 등에 대해 중점적으로 연구할 예정임
 - 특히 2007년 제2차년도 연구에서는
 - 우리나라 물류보안기본계획 수립 및 관련 법률 정비 및 제정에 관한 사항, 물류 보안 기술 및 장비 개발 및 국제 표준화 대응방안, 물류보안인력 양성 및 교육 프로그램 개발 등을 중점적으로 연구할 예정임

제1장

서론

1. 연구의 배경과 목적

1) 연구의 배경과 필요성

물류보안(supply chain security)이 새로운 국제규범으로 등장하고 있다. 눈에 보이지 않는 무역장벽으로 작용할 우려도 있는 것으로 분석되고 있다. 2001년 미국에서 일어난 9·11 항공기 테러 이후 각국과 국제기구에서 선박과 항만 등 물류 부문의 보안을 강화하면서 이 같은 현상이 나타나고 있다. 9·11 항공기 테러의 직접적인 피해국인 미국뿐만 아니라 다른 나라에서도 물류보안과 관련된 여러 가지 제도와 조치들을 도입하여 시행하고 있다.

미국의 경우 18개 정부 관련 기능을 통합한 국토안보부(DHS)를 2003년에 정식으로 출범시켜 보안 조직의 일원화를 꾀한 것을 비롯하여 해운보안법을 제정하면서 컨테이너 보안 협정(CSI)¹⁾과 대테러 민관 보안협력 프로그램(C-T PAT), 초대형 항만 방사능 탐지제도(Mega Port Initiative) 등을 도입, 물류부문의 보안을 강화하고 있다.

특히 미국은 이 같은 제도만으로는 자국의 국경을 효과적으로 보호하는데 한계가 있다고 판단하고, 최근에는 운수 부문의 모든 노동자를 대상으로 대대적인 신원조사에 착수하는 한편, 항만에 입출입하는 모든 근로자에 대해 생체

1) Container Security Initiative의 약자

인식이 가능한 신분증을 발급한다는 장기계획도 세워 놓고 있다. 또한 이 같은 시스템을 다른 운송 부문 근로자에 대해서도 확대할 예정이다. 지난 10월 13 일에는 항만보안법(SAFE Port Act)을 제정·공포하였다.

미국뿐만이 아니다. 국제해사기구(IMO)와 국제노동기구(ILO), 경제협력개발기구(OECD), 세계세관기구(WCO) 등 정부간 및 민간 국제기구도 미국과 유사한 제도를 도입하여 전 세계적으로 동일한 기준에 따라 물류 보안을 확대 하고 있다. 이 같은 국제기구를 통해 미국을 중심으로 도입된 보안기준이 글로벌 제도로 확대되어 정착되고 있다.

IMO의 경우 2004년 7월 선박 및 항만시설의 보안을 강화하는 이른바 ISPS Code²⁾를 도입한데 이어 2005년에는 선박과 해양시설 등에 대한 테러 예방과 진압을 목적으로 하는 새로운 협약을 채택하였다.³⁾ 특히 후자의 경우 해상테 러의 예방뿐만 아니라 선박을 테러의 수단으로 악용하거나 선박 등 해양 구조 물을 이용하여 대량살상무기(WMD)를 운반하는 것을 통제하는데 목적을 두고 있다.

OECD와 WCO,⁴⁾ 아시아·태평양경제협력위원회(APEC) 등 다자간·지역 간 국제기구도 해운·내륙·항공 등 모든 운송부문의 완벽한 보안 체제 확립 과 수출입 화물의 안전한 통관을 보장하는 새로운 제도를 도입하고, 각각 회원 국에 대해 시행을 촉구하고 있다. 이들 기구에서 도입하고 있는 보안제도는 기존 제도와 달리 물류 전반에 걸쳐 있어 앞으로 파급효과가 클 것으로 예상되고 있다.

그런데 문제는 현재 도입되고 있는 제도를 시행하는데 정부와 업계의 부담 이 커질 것으로 예상되고 있는 가운데, 각 나라와 국제기구의 물류보안 강화조

2) International Ship and Port Facility Security Code의 약자임.

3) 최근 IMO에서 채택된 2가지 국제협약은 “항해의 안전에 대한 불법행위의 억제를 위한 협약¹⁾(이하 ‘1988년 SUA 협약’)과 “대륙붕에 설치한 고정 해상 플랫폼의 안전에 대한 불법행위 억제에 관한 1988년 의정서”(이하 ‘1988년 SUA 의정서’)를 개정하는 것을 주요 내용으로 하고 있음.

4) WCO는 2005년 10월에 「국제교역의 안전과 간소화를 위한 국제기준(Framework of Standard to Secure and Facilitate Global Trade)」을 채택하고, 2007년까지 180개 회원국에서 시행할 계획임.

치가 앞으로도 더욱 지속될 것으로 전망되고 있다는 점이다. IMO의 경우 조만간 장거리 선박추적 시스템(LRIT)⁵⁾의 도입을 의무화할 예정이고, 미국은 항만보안법을 제정하면서 컨테이너 보안장비(CSDs)의 설치를 의무화하였다.⁶⁾

이와 같이 국제적으로 물류 보안 제도가 강화되고 있는 것은 테러 위협이 상존하고 있는데 따른 불가피한 조치로 인식되고 있다. 2001년 9·11 항공기 테러 이후 지금까지 크고 작은 테러 사고가 지구촌에서 빈발하고 있기 때문이다. 2002년 스페인에서 발생한 열차 폭발 사고, 같은 해 예멘에서 일어난 유조선 림버그 호 폭발사고, 이스라엘 애시 도드 항만에서 자행된 자살 폭탄사고 등이 대표적인 사례라 할 수 있다.

특히 전문가들은 테러리스트들이 항만이나 선박 등 물류 시설을 테러 대상으로 삼을 가능성이 매우 크다고 분석하고 있다. 항만을 공격하는 경우 배후에 도심이 위치하고 있어 테러 효과가 상대적으로 클 뿐만 아니라 수출입 물류를 일시에 마비시킬 수 있어 효과를 극대화하는 데 최적이라는 평가가 나오기 때문이다. 미국의 컨설팅 회사인 브즈 알렌이 분석한 ‘위 게임 시나리오’에 따르면, 테러로 항만의 기능이 모두 정지되는 경우 580억원의 불 가동 손실이 발생하는 것으로 추정하였다.

참고로 지난 2002년 미국의 서부 연안 29개 터미널이 근로자 파업으로 11일 동안 폐쇄되었을 당시 선박 200여 척과 컨테이너 30만 TEU가 처리되지 못하는 사태가 빚어 졌다. 이 같은 항만 폐쇄조치로 미국이 입은 경제적 손실은 4억 6,690만 달러로 추정되었다. 또한 항만 폐쇄가 4주 동안 계속되었을 경우에는 피해액은 더욱 불어나 모두 47억 달러의 손해가 발생할 것으로 추산되었다.

이에 따라 화물 공급 사슬에 걸쳐 있는 각종 물류 네트워크의 보안을 확보

5) Long Range Identification and Tracking System의 약자로, 이 시스템의 도입에 관한 규칙이 2006년 5월 IMO의 해상안전위원회(MSC)에서 기존의 해상인명안전협약(SOLAS 1974/78) 제5장(항해 안전) 개정 형태로 반영되었음. LRIT에 관한 규칙은 300톤 이상의 모든 국제항해선박에 2008년 1월부터 적용될 예정임.

6) 컨테이너 보안 장비(Container Security Devices)는 컨테이너가 운송되는 도중에 부정 개폐되는 것을 방지하는 장치를 말하는데, 미국의 록히드 마틴이나 제너럴 일렉트릭(GE)과 같은 글로벌 기업들이 이 사업에 참여하고 있음.

하는 것이 테러로부터 자국의 영토와 인명을 보호하고, 국가 경쟁력을 확보하는 핵심요소로 등장하고 있다. 즉, 현재화되고 있는 테러 공격으로부터 인명과 재산을 보호하는 것도 화급한 과제일 뿐만 아니라 다른 나라의 물류보안제도를 이행하지 않을 경우 심각한 물류 왜곡 현상이 일어날 가능성이 커진 것이 오늘의 현실이다.

미국은 이 같은 물류보안제도 도입을 통해 자국의 제도를 이행하는 국가에 대해서는 화물의 우선 통관을 보장하는 혜택(greenlane)을 부여하는 한편, 불이행국가에 대해서는 선박의 입항을 금지하거나 영해 추방도 불사한다는 입장을 고수하고 있어 향후 물류 부문의 보안 확보가 국가의 물류경쟁력을 좌우하는 중요한 변수로 작용할 것이 분명하다.

말레이시아와 컨테이너 허브 항만 경쟁을 벌이고 있는 싱가포르의 경우 미국이 도입한 컨테이너 보안 협정(CSI)을 세계에서 처음으로 시행, 물류 주도권 장악에 나서는 등 발 빠르게 대응하고 있는 것도 이 같은 움직임과 무관하지 않다. 또한 일본이 미국과의 협력 관계를 바탕으로 전자태그(RFID)를 부착한 이른바 ‘스마트 컨테이너’에 대한 실증 실험에 나선 것도 같은 맥락으로 풀이되고 있다.

이에 따라 각 구간마다 분절되어 있는 물류보안 시스템을 통합하고, 국제기준에 적합한 새로운 제도를 시행하는 것이 중요한 과제로 부각되었다. 특히 현재 미국과 국제기구 등에서 도입하고 있는 물류보안제도의 경우 이행을 지체하는 경우 무역장벽으로 작용할 가능성이 매우 크기 때문에 더욱 그러하다. 특히 기존 제도를 제대로 지키지 않는 경우 화물의 통관은 물론 선박의 입항이 거절될 수 있는 피해가 발생한다는 점에 유의할 필요가 있다.

2) 연구의 목적

물류보안은 우리나라에만 국한되는 현상이 아니라 다른 나라와 밀접하게 연계되어 운영된다는 특징을 갖고 있다. 또한 화물 공급 사슬(SCM)의 특성상 선

박이나 항만 등 단일 운송 모드는 물론 화물이 운송되는 모든 물류구간이 서로 유기적으로 연결되어 있다. 따라서 물류 보안에 관한 문제는 국내 제도뿐만 아니라 외국의 제도를 포괄적으로 검토하고, 대응 전략을 통합적인 관점에서 짜는 것이 매우 중요하게 되었다.

우리나라의 경우 정부 부처 간에 통합적으로 물류보안을 관할하는 정책이 없는 것이 가장 큰 문제점으로 지적되고 있다. 예컨대 상품을 만드는 제조업체에서 최종 소비자에 이르는 전 물류 과정을 통제하고, 보안을 확보해주는 제도가 우리나라에는 없는 것이 가장 큰 문제점이다.

또한 ISPS 코드에 따라 2004년 7월부터 항만보안에 관한 제도가 대폭 강화되었음에도 컨테이너 터미널에 입출입하는 트럭이나 승용차의 경우 통제가 거의 이루어지지 않는 것이 오늘의 실정이다. 선용품에 대한 통제 미흡이나 항만 출입증 발급 제도 등 앞으로 보완하여야 하는 점이 적지 않은 것으로 조사되었다.

각 항만에 설치되어 있는 폐쇄회로 TV도 관세청과 해양수산부가 각각 별도로 운영하고 있다. 관세청의 경우 밀수를 방지할 목적으로 이 같은 시스템을 설치한 반면, 해양수산부는 항만 경비 목적으로 시스템을 운영하고 있기 때문이다. 이 같은 중복 투자와 제도 운영에 따른 사각 지대는 곳곳에서 발견되고 있다.

항공 부문에서도 여러 가지 문제점이 있는 것으로 파악되었다. 예컨대, 항공보안을 담당하는 정부 조직이 미비할 뿐만 아니라 다른 부처와의 업무 협조와 의사소통에도 어려움이 있는 것으로 나타났다. 정부가 의욕적으로 추진하고 있는 이른바 상용화주 문제에 항공업계의 반대에 직면, 제자리를 찾지 못하고 있다.

외국에서 도입·시행되고 있는 물류 보안 제도에 대한 연구와 파급효과, 우리나라 물류 기업이나 국가 경쟁력에 미칠 영향 등에 대해서도 손을 놓고 있다 해도 과언이 아니다. 일본이나 싱가포르 등이 민간 부문과 협력 체제를 구축, 피해를 최소화하는 한편, 물류 보안 선도 그룹으로 나갈 장기 전략을 수립하고 있는 것과는 사뭇 대조적이다.

최근 해양수산부는 우리나라의 우수한 정보 통신 기술(IT)을 현재 도입되고 있는 물류 보안 제도와 결합, 물류 경쟁력을 높이고, 해외 상품화하는 한편, 환적 화물을 유치하는 전략을 추진하고 있다. 강화되는 물류 보안을 수세적인 관점에서 보지 않고, 항만 마케팅 전략으로 활용한다는 포석으로 풀이되고 있다. 해양수산부는 최근 국제적인 물류보안 강화 추세를 항만경쟁력 향상에 이용하는 전략도 추진하고 있다.

이 연구에서는 이 같은 관점에서 최근 각국과 국제기구를 중심으로 도입되고 있는 물류보안제도를 면밀히 분석하는데 일차적인 연구 목표를 두었다. 새로운 제도를 정확하게 이해하지 않고서는 대책 마련이 불가능하다는 판단에 따른 것이다. 그 다음으로 관심을 둔 사항은 우리나라 해운·항만·교통 등 물류부문이 안고 있는 보안 취약점이 무엇인지 확인하는 작업이기 때문이다. 외국의 제도와 내부의 강점과 약점을 동시에 파악해야만 앞으로의 대책이 나올 수 있다.

결론적으로 이 연구에서 궁극적으로 추구하고자 하는 목표는 다음과 같다.

첫째, 2001년 9·11 테러 이후 각국에서 시행하고 있는 물류보안제도를 정확하게 파악하고, 우리나라 기업과 정부가 어떻게 대응해야 하는지 분석한다.

둘째, 해운과 항만, 항공과 철도 등 우리나라 물류 네트워크에 걸쳐 있는 보안 취약점을 파악하고, SCM 차원에서 바람직한 대처방안을 제시한다.

셋째, 우리나라의 탁월한 정보통신기술을 기반으로 물류보안 네트워크를 구축함으로써 수출입 화물의 원활한 처리를 도모하는 한편, 물류보안 장비 및 시스템의 상품화 방안을 검토한다.

끝으로, 통합적인 관점에서 물류부문의 종합적인 대응방안을 제시함으로써 우리나라가 물류 핵심 국가로 성장할 수 있는 기반을 제공하는 데 연구의 목적을 설정하였다. 이 연구를 진행하는 과정에서 연구진들이 정부(해양수산부, 국가정보원, 건설교통부 등)의 관련 정책 수립에 적극 참여하고 있는 것도 이 같은 목적을 달성하기 위한 것이다. 연구보고서 말미에 제시된 제1차 연도의 연구 결론은 해양수산부와 공동으로 작업한 결과를 반영하였다.

2. 선행연구 내용의 분석

2001년 9·11 테러 이후 국제적으로 물류부문의 보안에 관한 관심과 우려가 크게 증폭되고 있으나 우리나라의 경우 이에 관한 연구는 거의 이루어지지 않고 있는 실정이다. 물류보안이라는 용어 자체가 아직 생소할 뿐만 아니라 보안에 관한 패러다임이 물류부문까지 확산되기 시작한 것이 바로 최근의 일이기 때문이다.

다만, 그 동안 각 국제기구나 국가에서 도입한 제도에 대해 소개하거나 분석한 보고서, 논문들이 일부 발표되고 있다. 국내에서는 국제해사기구(IMO)가 제정한 ISPS Code를 시행하기 위해 해양수산부가 관련 연구(「ISPS Code 시행방안 대비 국제협력 방안 연구, 2004」)를 수행한 바 있다. 이 연구는 특정 국제협약의 국내 이행절차를 마련하는 것에 연구를 초점을 맞추고 있다. 또한 같은 해양수산부가 용역사업으로 수행한 「ISPS Code 시행에 따른 항만보안관리제도의 제도적 개선방안, 2005」 연구도 나와 있다. 이 보고서는 부산항의 보안경비조직과 항만 보안료 징수체계를 개선하는 것으로 연구 내용을 한정하고 있다.

또한 한국해양수산개발원은 9·11 테러 이후 각국의 보안강화제도를 소개하는 KMI 현안분석보고서를 발표한 바 있다. 2002년과 2003년에 각각 발간된 ‘최근의 해사보안 강화 동향과 정책 시사점’과 IMO 해사보안협약 시행방안’등이 그것이다. 전자는 2001년 9·11 테러 이후 각 나라에서 도입·시행되고 있는 여러 가지 보안제도를 종합적으로 소개한 최초 보고서로 평가되고 있다. 후자는 국제해사기구(IMO)가 2002년 12월에 채택한 이른바 ISPS Code를 우리나라에서 시행하는데 필요한 정책적 시사점과 대응방안을 제시한 정책보고서이다. 해양수산부는 이 보고서를 토대로 선박 및 항만에 대한 보안전략 추진 계획을 수립하는 한편, ISPS Code를 수용한 고시를 제정하여 시행하고 있다.

〈표 1-1〉 선행 연구현황 및 선행 연구와의 차별성

구 분		선행연구와의 차별성		
		연구목적	연구방법	주요 연구내용
주요 선행 연구	1	- 과제명 : ISPS Code 시행방안 대비 국제협력 방안 연구 - 연구자(연도) : 전영우(2004) - 연구목적 : 국제해사기구에 서 제정한 ISPS Code의 국내 이행 절차 등에 관한 연구	- 문헌조사 - 해외 시행동향 조사	- IMO 및 타당사국 정부 통보관련 조치사항 - 외국 항만국 통제 대비·대응 요령 개발 - 보안선언과 인접 국가간 대체보안협정 체결 및 지역협력 방안 - ISPS Code의 국내 법률화 검토
	2	- 과제명 : ISPS Code 시행에 따른 항만보안관리체제의 제도적 개선방안연구 - 연구자(연도) : 목진용(2005) - 연구목적 : 우리나라 부산항의 항만 보안경비조직 개편 방안	- 문헌조사 - 해외 시행동향 조사 - 법률안에 대한 공청회	- 일본·중국 등의 항만 보안법률 - 선박 및 항만보안에 관한 법률 - 항만보안료 도입방안 - 우리나라 항만보안 관리체제의 제도적 개선방안
본연구		- 9·11 테러 이후 미국 등 주요 국가에서 시행하고 있는 물류 부문의 보안제도를 파악하고, 우리나라가 안고 있는 문제점이 무엇인지 검토한 후, 해운부문, 항만부문, 육상운송부문, 항공운송 부문에 대한 정책적 대응방안을 제시	- 문헌조사 - 해외 연구 동향 파악 - 국내 자료 분석 - 물류 부문에 대한 실태 현장 조사 - 전문가 중심의 자문 - 타 연구기관과 협동연구	- 우리나라 SCM 전 과정의 보안제도와 문제점 분석 - 외국의 관련제도에 대한 검토 - 테러 등으로 인한 물류 부문의 경제적 피해액 추정 - 물류 보안제도 미 이행에 따른 수출입 규제 등 무역 장벽 검토 - 우리나라 각 운송부문별 대책과 통합물류관점에서 바람직한 정부 대응 방안 제시

3. 연구의 주요 내용과 수행방법

1) 연구의 주요내용

이 연구는 올해와 내년까지 2개년에도 걸쳐 진행되는 과제이다. 이 같은 일정에 맞춰 연구 범위를 크게 둘로 구분하여 연구를 진행하고 있다. 연구 첫째년도인 올해는 주요국 등에서 도입되고 있는 물류 보안 제도에 대한 현황 파

악과 시사점 도출, 그리고 우리나라가 직면한 물류 보안 부문의 문제점을 분석하는 데 중점을 두었다. 연구 2차년도인 2007년에는 올해 수행한 1차년도 연구를 바탕으로 ‘국가 물류 보안체제 구축 세부 전략’을 수립하기로 하였다. 올해 진행되는 주요 연구 내용을 설명하면 다음과 같다.

〈표 1-2〉 주요 연구내용

연구년도	주요 연구 내용
2006년(1차년도) 연구	주요국의 물류 보안 제도 조사 및 분석, 시사점 분석
2007년(2차년도) 연구	국가 물류 물류보안체제 구축 방안 및 세부전략 작성 - 국가 물류보안 계획 수립 및 물류보안시장 선점전략 포함

제1장에서는 일반적으로 이루어지고 있는 사회과학 연구기법에 따라 연구 목적과 연구 내용, 그리고 연구 수행 방법 등에 대해 주로 언급하였다. 이 연구가 2개 년도에 걸쳐 진행되고 있는 점을 고려, 제1장에서는 1차년도와 2차년도의 연구 범위도 설정하였다.

제2장에서는 물류보안의 중요성과 취약요인 등에 대해 주로 언급하였다. 테러 등으로 물류 시스템이 단절되는 경우 우리 경제가 입을 손해뿐만 아니라 대외 교역 등에도 많은 영향을 미치기 때문에 이 부문에 많은 지면을 할애하였다. 그리고 제3장과 제4장과의 연결성을 확보하기 위해 제2장에서는 화물의 공급 사슬(SCM)에서 물류보안이 어떤 과정과 절차를 통해 확보되어야 하는지 구체적인 사례를 적시하면서 논술하였다.

그리고 주요국 및 다자간 국제기구에서 도입·시행하고 있는 물류 보안제도에 대해서는 주로 제3장과 제4장에서 고찰하였다. 9·11 테러 이후 글로벌 물류 보안제도를 주도하고 있는 미국은 물론 유럽연합(EU)과 국제해사기구(IMO) 등 국제기구의 관련 국제 규범 입법 동향에 대해서도 이 곳에서 구체적으로 검토하였다. 그리고 제3장과 제4장의 말미에는 각각 정책적 시사점을 적시, 우리나라 물류보안제도를 개선하는데 참조할 수 있도록 하였다.

제5장에서는 우리나라 물류 보안제도의 시행현황을 주로 검토하는데 역점을 두었다. 각 부처 별로 분산되어 시행되고 있는 보안 관련 제도를 분석한 다음 통합적인 관점에서 물류 보안을 효율적으로 확보할 수 있는 방안을 도출하는데 필요하기 때문이다. 특히 이 곳에서는 해운 항만 항공 등 각 물류 수단별로 구체적으로 어떠한 보안제도가 시행되고 있는지 파악하는데 주력하였다.

제6장에서는 해운과 항만, 내륙 등 물류 네트워크 전 분야에 걸쳐 현행제도의 시행에 따른 문제점, 외국의 물류 보안제도와 차이점 등에 대해 중점으로 분석하고, 향후 물류보안 정책 방향을 제시하였다. 우리나라 물류보안제도를 강화하는데 따른 선사와 화주 등 이해집단의 의견도 이 곳에서 반영하였다. 특히 이 곳에서는 현재 정부가 추진하고 있는 ‘국제물류혁신 및 브랜드 작업’ 등과 관련, 연계 방안을 모색하는데도 관심을 기울였다. 특히 제6장에서는 물류 보안과 관련하여 현재 사용되거나 개발되고 있는 장비와 기술, 시스템 등에 대해서도 검토하였다. 가장 중요하다고 판단되는 컨테이너 화물 검색기, 방사능 탐지기 등이 어떻게 설치되고, 운용되고 있는지 모두 이 곳에서 검토하였다.

제7장은 제1차년도 연구의 결론에 해당되는 부분이다. 2007년에 이뤄지는 제2차년도 과제 ‘국가 물류보안체제 구축 방안 및 세부 실천 전략’의 기본 방향이 주로 제시될 예정이다. 정책 제언도 이 곳에서 정리하여 제시하였다.

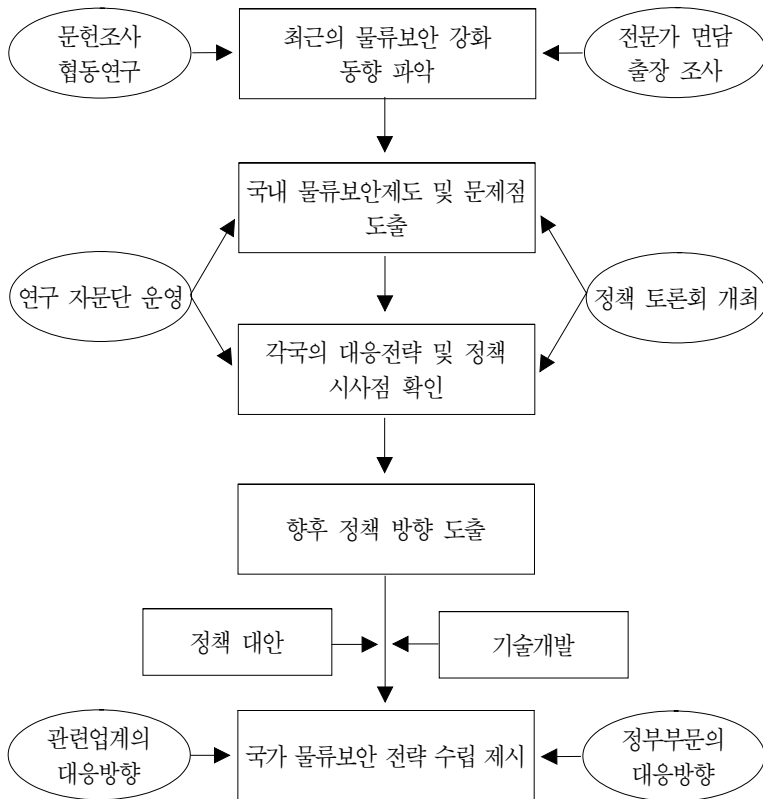
2) 연구 방법

물류보안제도는 우리나라에만 국한된 문제가 아니다. 상품의 제조에서부터 최종 소비자에 이르는 모든 물류 네트워크에 걸쳐 있기 때문에 국내뿐만 아니라 외국의 관련 제도도 우리나라의 수출입 화물 흐름과 물류 정책 전반에 적지 않은 영향을 미치는 것이 사실이다. 이에 따라 이 연구에서는 현재 물류 보안을 주도하고 있는 미국과 IMO 등 국제기구의 관련 제도와 동향에 대한 문헌조사를 우선적 실시하였다.

특히, 이 연구과제에 착수하기 전에 연구진들은 2001년 9·11 테러가 일어

난 이후 도입되기 시작한 물류 보안 관련 자료를 지속적으로 확보, 분석하면서 연구를 준비해왔다. 또한 최근의 물류 보안이 화물의 한 결절점(node)인 항만을 벗어나 물류 전 구간으로 확대되고 있는 점을 고려하여 지난 7월 6~7일 이틀 동안 APEC 주관으로 싱가포르에서 열린 ‘Total Supply Chain Security’ 심포지엄 자료를 확보하고, 전문가들의 의견을 수렴하였다.

〈그림 1-1〉 연구 수행 흐름도



둘째, 국내의 협동 연구체제를 만들어 연구를 수행하였다. 우선 일본에서 시행되고 있는 물류 보안 제도를 정확하게 이해하기 위해 일본과 중국 전문가에

게 원고 집필을 의뢰하였다. 제3장에 나와 있는 것이 그것이다. 또한 우리 연구진이 다루기에는 한계가 있는 항공 부문의 보안제도에 대해서는 한국항공대 유광의 교수를 협동 연구진에 포함하여 연구 내용의 질적 향상을 꾀하였다. 컨테이너 화물 검색기 개발 동향과 기술 등 물류보안 산업에 대한 부문은 EB 테크를 협동연구기관으로 선정, 원고 집필 및 내용에 대한 자문을 구하였다.

셋째, 산·학·연·정 협력 연구체제를 구성해 연구내용과 방향이 앞으로 정부는 물론 물류 기업이 정책이나 비즈니스 모델로 활용할 수 있도록 노력하였다. 특히 이와 관련하여 연구진의 일부는 해양수산부가 운영하고 있는 ‘국제 물류혁신 및 브랜드 작업’ 워킹 그룹에 참여하여 의견을 제시하는 한편, 여러 가지 의견을 수렴함으로써 연구 내용의 향후 정책 반영과 실용화에 역점을 두었다.

이 밖에도 이 연구가 여러 물류부문이 걸쳐 있고, 정책 측면뿐만 아니라 기술 개발 등에 관한 사항도 포함하고 있는 점을 고려, 학계·업계 등 다양한 분야의 전문가 그룹으로 구성된 연구자문위원회를 구성·운영하여 연구의 질적 수준을 제고하는 한편, 정부 정책 및 산업현장에서 활용될 수 있도록 최대한 노력하였다.

넷째, 해외 출장조사와 전문가 면담도 병행하였다. 유럽연합의 물류보안제도 시행 현황을 파악하기 위해 스페인의 주요 항만을 방문, 조사하였다. 아시아 권에서는 글로벌 컨테이너 화물 추적 시스템에 대한 실증 실험을 진행하고 있는 홍콩 및 중국, 그리고 일본을 방문, 연구 내용에 반영하였다. 또한 연구를 진행하는 과정에서 한국무역협회와 공동으로 2006년 10월에 ‘물류보안 토론회’를 개최하여 미국의 물류 보안 제도와 우리나라의 향후 대처 방안, 업계의 대응 방향 등에 대해서도 의견을 수렴하였다. 토론회에서 제시된 의견은 결론 부문에 반영하였다. 이 같은 연구수행방법과 절차로 그림으로 표시하면 위와 같다.

제2장

운송 수단별 테러와 보안 취약요인

1. 세계 정치 환경 변화와 테러

1) 동시다발적 테러의 발생

미국에서 동시 다발적인 테러가 발생한 2001년 9월 11일부터 세계의 정치와 외교 환경이 크게 변하고 있다. 새로운 형태의 전쟁도 시작되었다. 테러와의 전쟁이 바로 그것이다. 다른 국가의 위협과 공격을 격퇴하는 것이 국가 안보보장의 중요한 과제라고 생각하던 시대는 이미 과거사가 되었다. 공산주의의 붕괴로 소멸되었다고 믿었던 정치와 사상적 투쟁이 부활하였으며, 경제가 주역의 자리에서 전락하면서 패권 외교와 힘의 정치가 다시 부상하고 있다.

냉전과 마찬가지로 테러와의 전쟁에는 군사적 측면과 정치적 측면이 있다. 냉전에서 핵 군비와 대리전쟁이 중요한 역할을 한 것처럼 군사작전과 비밀공작활동이 테러와의 전쟁에서 중요한 열쇠가 될 것이라는 의견도 나오고 있다. 세계 물류보안제도를 쥐락펴락하고 있는 미국은 때로는 세계와 깊은 관계를 맺기도 하고, 때로는 자국의 형편에 따라 손을 빼기도 하는 이중적인 태도를 견지하고 있다.

이에 따라 전에는 미국이 세계를 필요로 하는 이상으로 세계도 미국을 필요로 한다는 전제가 존재하였다. 하지만 지금은 사정이 다르다. 미국은 필요하다면 독자적으로 전쟁을 수행할 수 있으나 테러와의 전쟁은 경찰 또는 군대와

정보기관의 양면 작전이 필요하다. 이는 한 나라만으로는 불가능하다. 지속적인 정보수집으로 테러조직의 아지트를 공격하거나 관계자를 체포하고, 테러단체로 들어가는 자금줄을 끊으려면 각국 정부의 적극적인 지원이 필요하다.

이 같은 정치 환경 변화는 사상 처음으로 세계가 미국을 필요로 하는 것처럼 미국이 세계를 필요로 하는 새로운 공식을 만들어 냈다. 9·11 테러사건 이후, 미국은 특정국의 군사적 위협을 대상으로 하던 종래의 안전보장전략을 전환하여 테러뿐만 아니라 ‘불량국가’와 같은 비대칭적 위협에 대처하는 한편, 테러리스트 손에 대량살상무기(WMD)가 들어가는 것을 차단하는데 역점을 두고 있다. 이 같은 정책을 추진하는 과정에서 미국은 전통적인 전쟁 억제전략에서 전환하여 예측이 곤란한 새로운 위협에 유연하게 대처하기 위해 정보능력을 확충하는 한편, 세계 전역에 배치한 미군의 변혁을 추진하고, 동맹국과 우호국과의 관계강화를 동시에 꾀하고 있다.

한편, 9·11 테러 이후 미국의 테러와의 전쟁은 지역에 따라 다른 형태를 취하고 있다. 아프가니스탄에서는 탈레반 정권이 타도되고, 알 카에다의 근거지가 파괴되는 한편, 현재는 파키스탄에서 탈레반과 알 카에다를 소탕하기 위한 작전이 이루어지고 있다. 이라크에 있어서는 미국의 공격으로 사담 후세인 정권이 붕괴되었다. 서유럽에서는 알 카에다 조직이 계속 적발되고 있으며, 예멘, 소말리아, 튀니지 등에서는 알 카에다와 그 동맹자인 이슬람주의 세력에 대한 비밀전이 행해지고 있다. 또한 동남아시아에서는 필리핀 정부가 미국의 군사원조를 받아 필리핀남부의 민다나오, 파시란 지역에서 아부 사얏에 대한 군사작전을 전개하고 있으며, 말레이시아, 싱가포르, 인도네시아에서는 제마 이슬라미아를 적발하고 있다.

2) 국제 사회의 테러 대책

문제는 국제사회의 지속적인 노력에도 불구하고, 테러와 테러 위협은 지속적으로 늘어나고 있다는 점이다. 최근 런던에서 영국 최초로 이슬람 과격파 소

행으로 보이는 지하철 동시 다발 테러가 발생한 것 외에 인도네시아의 발리 섬과 요르단에서도 대규모의 테러가 발생하는 등 테러 위협이 국제적으로 확산되고 있다. 특히 런던의 테러는 폭사한 실행범이 모두 영국 국적의 이슬람계 젊은이라는 점에서 관심을 모으고 있다. 이슬람 과격파가 선진국 이슬람 커뮤니티에 침투하고 있다는 사실에 전문가들은 주목하고 있다. 새로운 형태의 테러 공격이기 때문이다.

알 카에다를 비롯한 국제테러집단은 전 세계에 네트워크를 설치해 놓고 있다. 자살 테러공격의 가능성은 전 세계로 확대되고 있다. 아시아에서도 제마 이슬라미야와 아부 사얌 등 알 카에다 관련 테러집단이 활동하고 있으며, 인도네시아에서는 자살테러폭파사건이 자주 발생하고 있다. 필리핀도 예외가 아니다. 태국, 싱가포르, 말레이시아에서는 관련 테러리스트들이 체포되었다.

영국의 싱크 탱크 국제전략연구소(IISS)는 세계의 군사력을 분석한 보고서 ‘밀리터리 밸런스(2005년 판)’에서 동아시아 지역에서는 북한이 핵개발에 강한 의지를 확연히 나타내고 있으며, 중국이 군사력증강을 계속하고 있다고 강조하였다. 또한 국제 테러조직 알 카에다가 그 세력을 유지하고 있다고 분석하는 한편, 일본과 한국이 테러의 표적이 될 위험성이 있다고 전망하고 있다. 또한 이 보고서는 이슬람계 과격파 조직이 활발한 활동을 보이고 있지 않는 곳은 동아시아뿐이라고 지적한 다음 “한국과 일본은 미국의 동맹국으로서 테러의 잠재적 표적이 되고 있다”고 분석하였다. 알 카에다에서 훈련을 받은 잠재적인 테러리스트는 1만 8,000명 이상인 것으로 추정되고 있다.

21세기는 ‘테러의 시대’라고 평가할 정도로 테러와의 전쟁은 장기화되고 있다. 9·11 테러 이전에도 여러 건의 해상 테러 행위가 일어나는 등 테러 공격이 끝나지 않고 있기 때문이다. 해상에서의 테러는 1985년 크루즈객선 아킬레 라우로 호(ACHILLE LAURO) 사건이 효시이다. 그 이후 최근에는 2002년 중동-예멘 연안에서의 프랑스 국적 원유 탱커 림버그 호(LIMBURG) 폭파사건, 2004년 마닐라 만에서의 슈퍼 페리 14호 폭파사건이 일어났다. 이들 대부분이 선박이나 승무원, 여객을 표적으로 한 사건이다. 그러나 전문가들은 미국의 동

시다발 테러에서 항공기가 무기로 사용된 바와 같이 컨테이너선 등이 대량살상무기나 그 원재료 또는 테러리스트나 테러자금의 운송수단으로 사용될 우려도 증가하고 있다고 전망하고 있다.⁷⁾

2. 물류 공급망에서의 보안위협

1) 보안위협에 대한 현안

2001년 9·11 항공기 테러 이후 대부분 국가들은 테러리스트의 공격에 대한 자국의 취약성을 파악하고 대책을 마련하기 시작하였다. 이 같은 대책 가운데 먼저 항공운송시스템에 대한 보안대책이 우선적으로 이루어지고, 그 뒤를 이어 해상운송시스템, 내륙운송시스템 나아가 물류 전 구간으로 확대되기 시작하였다.

항공시스템에서는 세계 각국이 공항보안검색을 강화하고 있으며, 특히 피해 당사국인 미국은 국가 전반의 보안을 강화하기 위해 국토안보부를 설치하고, 대 테러에 관련 정책을 강도 높게 추진하고 있다. 미국은 2005년 4월 13일부터 입국하는 항공편 승객의 휴대품은 물론 탁송화물에 라이터와 성냥을 휴대 또는 탁송하지 못하도록 하고 있으며, 이를 어길 경우 벌금을 부과하는 법규를 시행하고 있다.

국제연합(UN) 산하의 전문기구인 국제민간항공기구(ICAO)⁸⁾는 국제민간항공조약의 부속서 형태로 국제민간항공의 안전 및 보안확보를 위해 가입국가가 지켜야 할 표준 및 권고사항을 제정하여 공표하고 이의 준수를 감사하는 활동을 하고 있다. 이에 따라 9·11 테러 이후 ICAO는 제3차 총회의 결의와 실천적 후속조치에 따라 국제민간항공조약 부속서 17에서 규정한 항공보안업무의

7) 이 부문은 일본 협동 연구과제(이카와 테츠오 집필) 내용을 수정, 보완한 것임.

8) International Civil Aviation Organization의 약자로, 국제민간항공의 안전, 질서, 효율적인 발전을 위해 설립된 기관임.

표준을 가입국가들이 준수하고 있는지 확인하기 위해 2002년부터 2008년까지 기간을 정해 놓고 1차적으로 감사 작업을 진행하고 있다.

항공보안에 있어서의 주요 이슈는 보안 수준향상을 위해 추가로 소요되는 보안비용 부담문제, 항공화물 보안문제, 감독기능과 검사기능 수행주체의 문제, 그리고 환승승객에 대한 검색 업무 책임문제 등으로 지적되고 있다. 항공 보안 비용 부담 문제에 대해 항공사들이 회원으로 되어 있는 국제항공운송협회(IATA)⁹⁾나 일부 학자 및 전문가들은 정부가 그 비용을 보조하여야 한다고 주장하고 있다.¹⁰⁾ 항공화물의 보안문제는 가장 취약한 문제로 지적되었는데, 사실상 공항에서 100% 검색이 거의 불가능하고 현실적으로 효과적인 보안대책을 수립하지 못하고 있는 실정이다.¹¹⁾ 항공보안업무는 감독관의 기능이 중요한 역할을 하는데, 미국은 정부기관, 유럽의 경우는 보안업무 수행업체와 동일한 조직에 감독관이 소속되어 있으나 우리나라의 경우 감독관과 보안업무를 수행하는 직원은 다른 기관에 속해 있다. 환승승객에 대한 검색의 경우 미국과 유럽은 공항당국이나 경찰이 수행하고 있으나 우리나라는 항공사가 책임을 지고 있다.

해상운송시스템의 보안에 대한 우려는 현재 국제화물의 많은 부분이 해상 컨테이너로 운송되는 특성을 갖고 있어 이에 대한 많은 관심들이 제기되고 있다. 직접적인 테러 피해국인 미국은 2001년 기준으로 미국에 등록되지 않거나 미국인 선원이 승선하지 아니한 약 5,400대의 선박이 전 세계적으로 무려 60,000군데의 항만에 입항한다고 지적하면서 해상운송 시스템을 활용한 테러 위협에 대한 우려를 강조하였다.¹²⁾

또한 Hecker(2002)와 Harrald 외(2004)는 오늘날의 항만이 다양한 기능을

9) International Air Transport Association의 약자임.

10) Online Air Transport World, www.atwonline.com, 2003년 6월 5일

11) ICAO, Aviation Security Training Package, Cargo(ASTP 123/Cargo), 2000; Goh, D., "Aviation security: Challenges and Opportunities", The Challenges of International Transportation Security, edited by Lawrence W. Lan, Institute of Traffic and Transportation, National Chiao Tung University, Taiwan, pp73-84, 2003.

12) APEC, J.S, "Strengthening international cooperation and technical assistance in preventing and combating terrorism", Intervention by APEC Secretariat the 12th Session of the Commission on Crime Prevention and Criminal Justice, pp16-19 May, Vienna, Austria, 2003.

수행하면서 운영에 있어서 복잡성을 띠고 있어 효과적으로 보안관리 수행에 어려움이 있다고 지적하기도 하였다.¹³⁾ 그리고 일반적으로 해상을 이용한 운송은 세계화물 거래량의 약 90%를 차지하고 있는데, 2003년 거래량은 2억 5,000만 톤으로 추정되었다. 이 가운데 겨우 2% 정도만이 목적지에서 실제적으로 검사를 받고 있다고 주장하면서 물류보안 위협에 대한 관심을 강조하였다.¹⁴⁾

해상 보안관리에 대한 주요 대상은 화물, 선박·항만시설, 그리고 선원, 즉 화물을 위장한 테러리스트 혹은 핵·생화학 폭발물 반입, 선박·항만시설의 무기화, 테러리스트를 지원하기 위한 가짜 선원 등으로 구분될 수 있다. 그리고 보안 위협은 선박등록의 불투명성이나 선박 소유권 문제에 대해서도 제기되고 있다(OECD 2003, ICS 1900¹⁵⁾). 현재 해운시장에서 편의치적(flag of convenience) 제도를 채택하고 있어 선박등록에 대한 세부적이고 명확한 지침이 부재할 뿐만 아니라 선박 소유를 익명으로 등록하는 것이 관행으로 이루어지고 있다. 이는 테러리스트에게 선박 소유를 익명으로 은폐케 함으로서 테러에 이용될 수 있는 가능성을 제공하기 때문이다. 따라서 보안을 확보하기 위해 선박을 운행하기 전에 선박의 소유, 등록 항만, 국적 등이 명확히 제시되는 것이 필요하다고 지적하고 있다.

또한 동남아시아 지역을 포함한 여러 지역에서 등장하고 있는 해적 행위에 대한 문제도 국제적으로 잘 알려진 보안 문제이다.¹⁶⁾ 국제해사기구는 2003년

13) Hecker, J.Z., *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, U.S. General Accounting Office, August 1, 2002; Harrauld, J.R., et al., "A framework for sustainable port security", *Journal of Homeland Security and Emergency Management*, Vol. 1(2), pp1-13, 2004.

14) Van de Voort, M. et al., *Security: Improving the Security of the Global Sea-Container Shipping System*, RAND, Europe, Report MR-1695-JRC, 2003; OECD, "Security in maritime transport: risk factor and economic impact, Maritime Transport Committee, Directorate for Science, Technology and Industry, July 2003.

15) ICS, *Course Notes: Ship Sale and Purchase*, Institute of Chartered Shipbrokers, London.

16) Richardson, M., "A time bomb for global trade: Maritime-related terrorism in an age of weapons of mass destruction", Viewpoint-Institute of South as Asian Studies, www.iseas.edu.sg/viewpoint, 2004; Jarvis, D.S.L., "The arc of instability: Regional security challenges for Australia and the Asia Pacific", Center for International Risk, The University of Sydney, 2003.

2분기에 발생한 화물탈취, 선원납치 및 살인, 파괴 등 45건의 해적 행위가 극동에서 발생했으며, 1993년부터 2003년까지 10년 동안 3,254건이 같은 지역에서 발생한 것으로 발표하였다.

물류보안을 강화하는데 들어가는 추가 비용문제가 또한 제기되고 있다. ISPS의 경우 선박식별, 보안계획, 경보시스템 등의 구축에 초기비용 198억 3,800만 달러(선사 1,170.6달러, 선박 757.4달러, 항만 55.8달러)와 연간 유지비용 7억 3,100만 달러(선사 725.6달러, 선박 4.3달러, 항만 1.6달러)가 소요되는 것으로 발표되었다(OECD 2003). 미국의 물류 보안 민관협력 프로그램인 C-TPAT의 경우는 협력 파트너 간의 시스템 구축에 소요되는 비용과 이에 필요한 인력훈련, 보안담당관 고용, 보안위험관리계획 수립, 운영비용 등 상당한 비용이 추가로 필요한 것으로 발표되었다.

2) 공급망에서의 테러 공격 및 방법

테러는 정치적, 종교적, 혹은 이념적 목적을 달성하고자 어떤 정부에 정치적 압력을 가하는 행동으로 정의된다. 운송시스템을 활용한 테러 공격을 통해서 정치적으로 압력을 행사하는 형태는 크게 두 가지로 나누어질 수 있다. 첫째, 대량의 인명피해나 운송 인프라에 손상을 줌으로써 대중매체를 통하여 공포나 국민의식에 영향을 끼치는 방법이다. 둘째, 물류 인프라의 파괴를 통해서 장기간 동안 물류흐름의 방해를 일으킴으로써 경제적 손상을 가하는 방법이다. 이러한 테러의 특징은 가용한 정보의 제약으로 예측이 거의 불가능하며, 이로 말미암아 피해가 크다는 데 문제의 심각성이 있다.

운송시스템을 활용한 테러 공격은 전 공급망에서 특정부분의 취약성과 밀접한 관계가 있으며, 인명 피해와 경제적 피해를 발생시킬 수 있다. 공급망에서의 테러 대상은 크게 세 가지로 나누어 질 수 있다. 첫째는 물류 인프라로서 화물 운송에 사용되는 모든 시설을 말한다. 둘째는 물류시설 운영 측면으로서 화물의 흐름을 통제하는 모든 활동이 포함된다. 셋째는 화물 그 자체로서 물류

망의 흐름에 따라 실제로 움직이는 실체를 의미한다. <표 2-1>은 운송 모드별로 잠재적 테러의 공격 대상을 요약한 것이다.

〈표 2-1〉 운송모드별 테러 공격 대상

구 분		운송 모드			
		해상	항공	철도	도로
물 류 인프라	운송로	해상로	항공로	철로 터널 다리 교차로	도로 터널 다리 교차로
	환적 장소	항만터미널	공항터미널	화물터미널 철도정차 야드	물류터미널
시설 운영	통제 시스템	해상운송 관리 시스템	항공운송 시스템	중앙 통제소 지방 통제소	도로 운송관리 시스템
	통신 시스템	통신망	통신망	신호체계	통신망
	종업원	선원 하역인력 보수인력 정보처리 인력	승무원 하역인력 보수인력 정보처리 인력	기관사 하역인력 보수인력 정보처리 인력	운전수 하역인력 보수인력 정보처리 인력
	운송수단	선박 바지	비행기	화차 차량	트럭 트레일러
운송 화물		비위험화물 폭발화물 유독물 가연화물	비위험화물 폭발화물 유독물 가연화물	비위험화물 폭발화물 유독물 가연화물	비위험화물 폭발화물 유독물 가연화물

자료 : 한국해양수산개발원

역사적으로 실제로 사용된 테러 방법은 다양하다. 인화성 물질을 이용한 방화, 폭발물 사용, 극약이나 생화학 약품 살포 등이 전형적이다. 그러나 현재 가장 큰 위협으로 인식하고 있는 것은 핵폭탄, 납치, 물리적 차단, 사이버 범죄 등으로 요약할 수 있다. 테러리스트들은 운송수단에 폭발물을 설치할 수 있도록 훈련된 지상요인에서부터 영공이나 해상에서 테러공격을 감행할 수 있는 고도의 훈련된 특수요원까지 다양하다.

항공기에 대한 테러는 1960년대 중반부터 정치적 수단으로 항공기 납치 및

승객들에 대한 테러가 본격화되면서 국제문제로 부각되었다. 특히 1968과 1972년 사이에 절정을 이룬 항공기 납치는 1969년 한 해 동안 85건이 일어나 주당 2건이 발생한 것으로 분석되었다.¹⁷⁾ 그 후 1970년대 중반부터 테러행위는 점차 감소하는 경향을 보이고 있다. 세계 각국이 공항과 항공기에 대한 보안시설 강화 그리고 탑승객과 적재화물에 대한 보안 검색 장비를 개발하고, 검색 수준을 높여 항공 테러를 사전에 차단하고자 노력했기 때문이다. 그럼에도 불구하고 국제적인 상황 변화와 국가간 이념, 이해 관계대립 등으로 테러는 계속되고 있다. 9·11 이후에도 2004년 8월 24일 러시아 영역에서 러시아 여객기 2대가 거의 동시에 추락한 사건은 테러에 의한 것으로 확실시되었다. 모스크바를 출발한 T-154 여객기는 러시아 휴양지인 소치로 향하다 로스토프에서 추락했으며, 납치사실을 알리는 위험신호를 3차례 관제탑에 보냈던 것으로 알려졌다. 또한 레닌그라드로 운항하다가 추락한 T-134기 사고도 러시아 당국은 이슬람 단체의 소행이라고 주장하였다.¹⁸⁾

〈표 2-2〉 테러 방법

	테러 방법	설명
1	화재	인화성이 강한 물질을 이용한 방화
2	30kg 미만의 TNT 폭파	사람이 휴대할 수 있는 용량의 폭파
3	30kg TNT 폭파	소형 차량을 이용한 폭파
4	3000kg TNT 폭파	대형 차량을 이용한 폭파
5	극약	독약 살포
6	생화학	생화학 물질 살포
7	테러 위협	폭파 정보와 같은 공격
8	핵폭파	핵폭탄을 이용한 파괴폭파 공격
9	핵 먼지	핵방사에 의한 파괴 공격
10	납치	불법에 의한 감금
11	물리적 차단	물리적 장애물을 이용한 범행
12	사이버 범죄	컴퓨터 시스템 해킹

자료 : OECD, *Container Transport Security Across Modes*, 2005

17) 최진태, 「테러, 테러리스트 & 테러리즘」, 서울: 대영문화사, 1997.

18) 동아일보, 2004년 8월 18일 : A11면

현재까지 알려진 최상위의 해상 테리그룹은 1980년 이후 스리랑카 정부를 상대로 전쟁을 하고 있는 LTTE(Liberation Tigers of Tamil Eelam; 타밀엘람해방호랑이)이다. 그들은 1990년 7월부터 스리랑카 해군을 타겟으로 40회 이상의 해상 자살공격을 수행해왔다. 그들은 또한 스리랑카 해상에서 외국의 민간 선박들을 대상으로 공격, 납치, 파괴 등의 행위를 해오고 있다. 다른 테리 그룹인 JI(Jemaah Islamiyah)는 2001년 후반 미국의 관심을 끌기 위하여 미해군 군함을 타겟으로 공격할 계획을 세웠다. 하지만 이 계획은 싱가포르 JI 멤버들의 공격착수 수행능력의 부족으로 실패로 끝났다. 필리핀에 작전기지를 둔 ASG(Abu Sayyaf Group)는 외국인을 유괴하고 협박, 제거, 암살 등을 해왔다. 2000년도 말레이시아의 Sipadan 휴양 섬에 여행 온 외국 여행객 21명을 납치한 다음 일년 후 150만 달러를 받고, 인질을 풀어주었다. 그 후 2001년 Palawan 섬에서 여행객 20명을 납치 하여 미국 시민을 포함한 일부 여행객을 살해하였다. 또한 M/V 슈퍼 페리 14호는 2004년 2월 27일 마닐라만을 떠난 직후에 폭파되어 100명 이상의 승객이 피살되었다.

3) 운송시스템에서의 보안 위험

운송시스템에서의 보안 위험은 크게 두 가지로 구분된다. 첫째, 인프라 보안 위험은 공급망의 물류 흐름을 방해하는 목적으로 테러범이 인프라에 손상을 입히거나 파괴하는 것을 의미한다. 둘째, 공급망 보안 위험은 공급망의 운송 수단, 즉 트럭, 선박, 항공기 등에 다양한 폭발물을 은폐시켜 운송하거나 위험 화물을 대상으로 테러범이 원하는 시설을 파괴 및 사상자를 발생시키는 위험을 의미한다.

특히, 해상운송에 있어서의 물류 왜곡은 경제적 활동뿐만 아니라 세계 무역에 상당한 영향을 미치는 것으로 인식되고 있다. 미국의 경우 지속적인 테러 위협으로 투자가 GDP의 2% 가량 감소한 것으로 분석되고 있다(Saxton

2002).¹⁹⁾ 또한 향후 발생할 우려가 있는 테러에 대한 부정적 영향력도 선진국 뿐만 아니라 개발도상국에서도 작용하고 있는 것으로 나타났다. 예로서 APEC 지역에 있는 일부 국가는 해상운송의 테러에 대한 취약성과 지속적으로 발생하고 있는 해적행위로 말미암아 외국인 직접투자가 감소한 것으로 나타났다.²⁰⁾

(1) 인프라 보안 위협

물류 인프라에 대한 테러 공격 대상물은 철도/도로의 터널, 철도/도로의 다리, 복합운송 터미널, 물류 터미널, 항만 터미널, 철도 정차 야드, 교통 통제 관리 시스템, 철도 시스템이 전원 공급기지, 수로 등이 될 수 있다. 물류 인프라에 대한 테러는 운송의 연계 부분을 마비시킴으로 인해 물류 흐름에 영향을 끼치고, 결과적으로 우회, 지체, 운송 형태의 전환을 발생시킨다. 이때 경제적 손실은 추가 운송비용과 파괴된 시설의 재건 비용으로 추정된다. 추가 운송비용은 파괴된 시설에서 처리하는 화물의 물동량과 종류, 대체 운송수단 유무, 복구시간 등에 따라 달라진다.

(2) 공급망 보안 위협

공급망 위협은 테러범이 공급망을 악용하여 테러를 시도하는 것을 의미하고, 이 경우 운송 시스템은 테러의 대상이 아니고 수단이 된다. 공급망을 악용한 피해는 크게 두 가지로 분류된다. 먼저, 운송수단, 즉 트럭, 선박, 항공기 등은 공급망을 통해서 전 세계로 다양한 화물을 운송한다. 이 화물은 원료를 포함해서 완제품, 반제품 등이 소비자에게 이송되기까지 다양한 시설과 장소, 즉 산업단지, 물류센터, 그리고 인구가 밀집한 지역을 통과하게 된다. 이 때 운송수단뿐만 아니라 화물은 테러범이 폭발물이나 독극물을 은폐하는 장소로 활용되

19) Saxton, J., *The economic costs of terrorism*, Joint Economic Committee, United States Congress, Washington D.C., 2002.

20) Commonwealth of Australia, *Costs of Terrorism*, Economic Analytical Unit, Department of Foreign Affairs and Trade, 2003.

어 그들이 원하는 장소에서 피해를 가할 수 있다. Abt Association Inc.는 이러한 종류의 피해 분석 연구를 실시하였는데, 이 보고서에 따르면 미국의 항만에 단일 핵폭탄 공격과 생화학 공격이 가해졌을 때 인적·경제적 피해는 <표 2-3>과 같이 나타나는 것으로 추정되었다.

〈표 2-3〉 보안 위험 피해 예측

구 분	핵폭탄 공격	생화학 공격
사상자 수(명)	50,000 ~ 1,000,000	30,000 ~ 3,000,000
재산 손실(달러)	500억 ~ 5,000억	10억 ~ 100억
무역 직접 손실액(달러)	1,000억 ~ 2,000억	200억 ~ 2,000억

자료 : Commonwealth of Australia, *Costs of Terrorism*, Economic Analytical Unit, Department of Foreign Affairs and Trade, 2003.

다음으로 위험화물, 즉 가연성 가스나 독극물 탱크를 활용한 테러이다. 이때 테러범은 특별히 폭발물이나 생화학 폭탄을 은폐하여 이동시킬 필요 없이 위험화물 자체가 밀집 인구지역, 터널, 다리, 혹은 주요 건물 이동하므로 쉽게 공격 대상으로 활용하여 대량의 사상자와 경제적 피해를 발생시킬 수 있다. 예를 들면, LPG 40톤이 폭발되었을 때 반경 150m 내에서는 건물 파괴와 사상자가 발생되었으며, 반경 300m 내에서도 사상자 발생, 반경 500m는 치명적 부상자가 발생하는 것으로 분석되었다. 또한 가솔린 1,000kg이 방출되었을 때 바람의 영향 없이도 약 200명의 사상자가 발생하고, 바람이 있을 경우 약 1,000명의 사상자가 발생하는 것으로 분석되었다. 역사적으로 인도의 보팔(Bhopal)에서 메틸 이소시안산염이 탱크에서 누출되어 사상자가 거의 4,000명에 육박하였다. 그리고 1978년 7월 11일 스페인 산카로스에서 발생한 무색의 가연성 가스인 프로필렌이 폭발되었을 때 217명의 사상자가 발생하였다.

3. 물류보안 취약 요인 분석

1) 물류 공급망의 주요 활동 주체

공급망에서 활동하고 있는 주체들은 역할에 따라 크게 다섯 그룹으로 나누어진다(<표 2-4> 참조). 그러나 단순 운송업자들이 물류 서비스 영역을 확대하여 일괄운송서비스 제공자로 전환되는 추세에 따라 명확한 구분을 하기가 사실은 어렵다.

화물운송은 매도인과 매수인 사이의 거래에서 발생한다. 물류보안 입장에서 매도인은 공급망에서 중요한 역할을 담당하고 있다. 매도인은 컨테이너에 선적될 화물에 대한 정보뿐만 아니라 화물의 운송 경로에 대한 정확한 정보를 가지고 있기 때문이다. 즉 매도인은 화물을 컨테이너에 선적, 잠금장치를 한 다음 봉인하여 매도인의 작업장에서 매수인에게 화물을 보내는 작업을 한다.

컨테이너 보안의 분석은 바로 매도인의 작업장에서 화물을 컨테이너에 선적하고 봉인하는 시점부터 시작된다. 봉인된 컨테이너는 매도인과 매수인의 무역계약 즉 화물에 대한 권리이전 시기, 위험부담 및 비용부담의 분기점, 화물의 인도장소, 운송계약 및 보험계약의 체결의무에 따라 이동을 한다. 따라서 화물의 보안은 화물이 출발하는 매도인의 공장에서 매수인의 창고에서 소비되는 시점까지 유지되어야 한다.

화물의 물리적 이동을 위해 공급망에서 크고 작은 많은 운송관련 주체들이 참여한다. 보안 측면에서 참여한 주체들이 증가하면 증가할수록 보안 확보 노력은 더 요구된다. 이러한 노력은 먼저 매도인이 보안 확보를 위해 화물 이동에 참여하는 운송주체들과의 정보 공유가 중요하다. 왜냐하면 운송주체들은 상대적으로 화물에 대한 정보가 매도인보다 부족하기 때문이다. 또한 공급망에서 포워더도 보안 확보에 중요한 역할을 한다. 포워더는 매도인에게는 운송인의 역할을 하는 반면 운송인에게는 화주의 대리인 입장에 있다. 즉, 이들은 적절한 운송수단을 선택하여 운송에 따르는 일체의 부대업무를 처리해 주는 기능을 하고 있다.

현실적으로 포워더는 화물의 추가 비용이 요구되는 보안 확보에 관련된 번거로운 작업을 꺼려하는 입장에 있다. 또한 단거리 운송에 참여하는 많은 중소기업들은 효과적인 보안확보를 위한 장비나 능력을 갖추지 못하고 있는 실정이다. 일반적으로 공급망의 보안확보 역할을 보면 운송 관련기관은 운송수단, 운전기사, 시설 등에 대한 책임을 담당하고, 세관은 컨테이너에 내장된 화물에 대한 책임을 담당하고 있다. 이와 같이 물류 활동 주체가 많은 것은 역설적으로 테러리스트들이 비집고 들어갈 틈이 많다는 점을 의미한다. 다음 <표 2-5>에서 보는 바와 같이 현재 국제적으로 시행되고 있는 여러 가지 물류보안제도는 이 같은 허점을 메우기 위한 국제사회의 결집된 노력을 보여주는 것이라고 할 수 있다.

<표 2-4> 공급망에서의 활동 주체

역할	활동 주체
고객	매도인(제조업자, 수출업자 등)
	매수인(인수자, 수입업자 등)
상거래 지원	구매대리점
	운송인 혹은 NVOCC
	관세사
운송	공컨테이너 저장 운영자
	창고 운영자
	내륙 터미널 운영자
	도로 운송업자
	철도 운송업자
	바지 운송업자
	해상 운송업자
	항만 운영업자
	기타 항만서비스 운영업자
기관	운송 관련 기관
	세관
	수출입 면허 기관
	항만국
	수출입 통계기관
	기타 외교통상부, 무역협회 등
재정	은행
	보험업자

자료 : 한국해양수산개발원

〈표 2-5〉 각종 물류보안제도의 특징

구 분	컨테이너 검사	컨테이너 무결성	컨테이너 환경	컨테이너 트래킹	컨테이너 정보
국제 기구					
IMO	○		○		○
ILO			○		○
WCO	○		○	○	○
ISO	○	○			
EU		○	○		○
APEC/STAR	○			○	○
UN-ECE/TIR	○	○			○
UN-ECE/International carriage of dangerous goods	○	○	○		
개별국가					
CSI(미국)	○				
C-TPAT(미국)		○	○		○
24 Hours Rule(미국)	○				○
Bio-Terrism Act(미국)	○				○
산업계					
BASC		○	○		○
E-Business MoU					○
IRU	○	○	○	○	○
OSC(미국)	○	○		○	
SST(미국)	○		○	○	

자료 : 한국해양수산개발원

2) 물류 공급망의 취약점

21세기는 세계시장의 글로벌화에 따라 정치, 경제를 비롯해서 인류의 모든 생활이 급변하고 있다. 글로벌화된 시대에는 공급업자, 생산공장, 물류기지, 판매시장 등이 넓은 지역과 여러 나라에 걸쳐 분포되어 있다. 이에 따라 기업들은 글로벌 생산 및 분배 환경의 치열한 경쟁에서 살아남기 위해 글로벌 공급망 관리의 필요성을 더욱 인식하고 있다. 이러한 글로벌화는 기업과 국가에게 최초 원재료 공급에서 소비자까지 전 세계의 물류흐름에서 보안을 확보하면서 효율적으로 관리해야 하는 어려움을 주고 있다. 현재의 글로벌 경제 구조에서

물류보안을 확보하는 문제는 쉬운 작업이 아니다. 화물의 시작점에서 목적지까지 흐르는 공급망에 많은 국가들이 참여하고 있고 다양한 운송모드를 사용하고 있기 때문이다. 더욱이 공급망을 구성하고 있는 다양한 기업, 즉 생산기업, 운송업자 등으로부터 운영시스템, 법적 문제까지 거미줄 같이 얽혀 있기 때문이다. 결과적으로 가장 큰 어려움은 국제적으로 복잡하게 이동되고 있는 화물을 통제할 수 있는 단일 보안 시스템이 부재하다는 것이다.

(1) 항만/공항의 취약성

항만/공항은 내륙운송 시스템과 연계되어 있을 뿐만 아니라 다양한 저장 시설을 갖추고 있어 본질적으로 테러의 공격에 많은 취약성을 가지고 있다. 또한 주요 도시에 위치하고 규모나 접근성에서 테러 공격의 가능성은 크다고 할 수 있다. 이러한 항만/공항은 공급망에서 화물의 내륙 운송시스템의 연결점으로서 중요한 역할을 담당하고 있다. 특히 대량의 화물을 처리하고 있는 주요 항만/공항이 테러 공격을 당할 경우 운송업자나 화주는 대체 경로를 이용함으로써 발생하는 추가 비용 부담에 따른 경제적 손실을 가져오게 된다.

항만은 접근성 측면에서 공항보다 용이하여 보안관리가 더 어려운 특성이 있다. 연간 수백만 TEU에 달하는 컨테이너 물동량을 처리하는 항만에서 모든 화물에 대해 전수 검사를 수행하는 작업은 거의 불가능하다. 따라서 견본 검사를 수행하는 방법에도 한계가 있으므로 화물에 대한 정확한 정보, 항만의 특성, 화주, 수출업자, 운송업자들 간의 정보공유는 필수적이라 할 수 있다. 현재 컨테이너에 이용되는 봉인 방법은 단순히 물리적으로 컨테이너의 개봉 여부만 확인하는 것으로 항만/공항에서 테러의 목적으로 사용될 가능성은 크다. 예를 들면, 테러에 사용할 목적으로 화물의 교체 투입, 위조 컨테이너 선적, 포장 작업 시 위해 물질 투입, 공 컨테이너에 폭발물 투입 등 다양한 방법이 존재한다.

(2) 정보 및 서류의 취약성

운송에 사용되는 각종 서류 또한 쉽게 위조할 수 있다. 현재의 과학 기술로

문서 위조는 상대적으로 쉽게 이루어 질 수 있으며, 충분한 검증 없이 위조된 서류를 이용하여 선박의 항로를 조정할 수 있다. 그 한 예로서 ‘유령선박’을 들 수 있다. 유령선박은 해적에 탈취되어 선원들은 피살되거나 해상에 버려진 뒤 개조된 선박이다. 또한 탈취한 선박의 이름을 변경하고 서류를 조작하여 여러 항만을 항해할 수 있다. 이러한 유령선박은 해상에서 다양한 범죄에 사용되고 있는 실정이다. 미국에서 발생한 9·11 항공기 폭파 사건도 테러리스트들이 위조 신분증을 이용하여 항공기에 탑승한 후 승무원을 납치하여 생겨난 사건이다.

(3) 승선 인원의 취약성

해상운송의 경우 최근의 선박들은 다양한 과학기술의 발달로 20명 내외의 선원이 승선하고 운항한다. 이러한 소규모의 인원은 선박의 보안 확보에 취약성을 내포하고 있다. 만일 소규모의 선원이 항만에 정박하여 많은 양의 화물 처리 작업에 투입될 경우 외부인의 침입을 감시할 여유가 없어 선박 및 컨테이너 보안문제는 의외로 심각하다.

또한 외항선의 경우 선박에서 작업하는 선원들은 다양한 국적을 가지고 있어 현실적으로 이들의 신원조사를 면밀히 검토하는 것은 거의 불가능하다. 선원 신분증을 쉽게 위조할 수 있는 것도 문제점으로 지적되고 있다. IBM에서 발표한 선원의 신분증에 대한 위조 여부에 대한 보고서에 따르면, 54개 해운업체를 대상으로 선원의 신원조사를 수행한 결과 1만 2,000명 이상이 위조 자격증을 소지하고 있는 것으로 나타났다.

(4) 운송수단의 취약성

해상운송에서 선박이 속도를 낮추어 좁은 해로를 항해할 때 테러 공격의 대상이 된다. 또한 선박 통행량이 많은 지역에서도 선박이 활동할 수 있는 반경이 상대적으로 적어 테러 공격에 적절히 대응할 수 없는 상황도 발생한다. LNG/LPG 선박의 경우 인화성이 큰 물질을 적재하고 있기 때문에 그 자체가

테러 공격의 대상이 되고 폭발시 심각한 사태를 유발시킬 가능성도 있다. 또한 가솔린이나 디젤과 같은 휘발성이 강한 유류를 실어 나르는 선박은 그 자체가 폭발물이 될 수 있기 때문에 테러 공격에 각별한 주의가 요구된다.

제3장

국제기구의 물류보안제도와 시사점

1. 국제해사기구(IMO)

1) 솔라스(SOLAS)협약 개정

(1) 개정 배경 및 개요

국제해사기구 본부에서는 ‘1974년 국제인명안전협약(이하 ‘SOLAS협약’이라 함)’²¹⁾ 개정을 위한 외교회의가 2002년 12월 9일부터 13일까지 개최되었다. 개정내용은 해상보안을 강화하기 위한 규정을 SOLAS협약에 포함하기 위한 것이었는데 SOLAS협약 제V장의 AIS장비의 조기 탑재 추진과 SOLAS협약 제XI-1장 및 제XI-2장의 해상안전 및 보안특별조치가 핵심을 이루고 있다. 이 중 제XI-2장은 선박 및 항만시설의 보안에 관한 규칙(이하 “ISPS Code”라 한다)²²⁾을 포함하고 있다. 원래 SOLAS협약은 해상에서 인명의 안전을 증진할 목적으로 선박의 설비, 구조 및 운항요건 등을 규정한 것이다. 그러나 이번 개정에서 포함된 해상보안에 관련한 규정은 선박 및 항만시설 종사자의 상호 협조로 해안보안을 위협하는 행위를 식별해서 저지하는 것을 목적으로 하고 있어 종래의 입법 목적과는 상이한 내용이다. 개정협약에 포함된 해상테러 방지를 위한 규정들은 9·11테러 이후 해상테러방지에 혼신의 노력을 기울이고

21) 정식명칭은 “International Conference on Safety of Life at Sea”임.

22) 정식명칭은 “International Code for the Security of Ships and of Port Facilities”임.

있는 미국의 강력한 요구에 국제사회가 마지못해 수용했다고 하여도 과언이 아니다.²³⁾ SOLAS협약은 개정된 내용의 발효에 관하여 이른바 ‘묵시적 수락 절차’ 즉, 협약 개정에 대하여 체약국의 명시적 반대가 없으면 일정 기간 후 발효되는 절차를 취하고 있다. 이에 따라 개정협약은 채택일로부터 1년 6개월 후인 2004년 7월 1일에 발효하였다.

(2) SOLAS 제V장의 개정내용

SOLAS 제V장의 개정부분은 선박 자동 식별 장치(Automatic Identification System, AIS)의 선박탑재 시기를 앞당긴 것이다. 개정 전에는 2005년 7월에서 2007년 7일까지 탑재하도록 한 것을 2004년 7월로 앞당겼다.

〈표 3-1〉 AIS 탑재시기

구 분	개정전 기한	개정후 기한
총톤수 300톤 이상 3,000톤 미만	2005. 7. 1	2004. 7. 1이후 첫 검사일 또는 2004. 12. 31 중 빠른 시기
총톤수 3,000톤 이상 1만톤 미만	2006. 7. 1	
총톤수 1만톤 이상 5만톤 미만	2007. 7. 1	

주 : 여객선 및 유조선은 제외

이는 동 선박들이 국제항행에 종사한다는 점을 고려하여 여객선 및 유조선 이외의 총톤수 300톤 이상 5만톤 미만 선박의 AIS 탑재시기를 ISPS Code의 발효시기인 2004년 7월 1일에 맞추기를 요구하였기 때문이다. 그리고 설치한 AIS는 항상 작동 상태로 유지할 의무도 부과하였다.

(3) SOLAS 제XI-1장의 개정내용

SOLAS협약 제XI장의 제3규칙인 선박식별번호(Ship Identification Number) 규정의 적용시기를 앞당기고, 선박이력기록부(Continuous Synopsis Record,

23) 해양수산부, “ISPS Code의 국내수용방안연구”, 2003.7, p.15.

CSR)를 제5규칙으로 신설하는 개정을 하였다. 선박식별번호는 기존협약에서도 총톤수 100톤 이상의 모든 여객선과 총톤수 300톤 이상의 모든 화물선에 대해 표시를 의무화하고 있었다. 개정협약은 그 적용시기를 앞당겨서 2004년 7월 1일 이전에 건조된 선박은 2004년 7월 1일 이후 첫 번째 도래하는 입거기간까지 설치하도록 하였다. 선박이력기록부는 선박이 해적의 대상이나 테러행위에 이용되지 않도록 선박의 이력을 추적할 수 있는 사항 즉, 기국명, 기국등록일자, 선박식별번호, 선박명, 선적항, 선박소유자 이름 및 주소, 나용선자 이름 및 주소, 회사명/주소 및 안전관리회사명, 선급명을 기재하도록 되어 있다. 주관청은 총톤수 500톤 이상의 화물선에 대하여 선박이력기록부를 발행하고, 2004년 7월 1일 전에 건조된 선박은 2004년 7월 1일부터 동 기록부를 유지하여야 하며, 기록내용이 변경된 경우는 주관청이 3개월 내에 재발행하여야 한다.

(4) SOLAS 제XI-2장의 개정내용

해상테러방지를 위한 해안보안규정을 반영하기 위하여 신설된 규정이다. 총 13개 규칙으로 이루어져 있으며, 세부사항은 별도로 채택된 국제 선박 및 항만 보안에 관한 규칙(ISPS Code)에 위임하고 있다. 주요내용은 다음과 같다.

① 적용대상(제2규칙)

해상보안특별조치 대상은 여객선(고속여객선 포함), 총톤수 500톤 이상의 화물선(고속 화물선 포함), 이동식 해양구조물, 국제항해에 종사하는 선박과 관련된 항만시설이다.

② 관계자의 의무(제4규칙 및 제5규칙)

자국선박, 자국영토내 항만시설, 자국에 입항하는 선박에 대한 보안과 관련하여 체약국의 의무와 선사 및 선박의 준수사항을 규정하고 있다. 선박은 ISPS Code 준수 여부를 심사받아서 그 증서를 소지하여야 하고, 선사는 체약

국 점검시 선박소유권의 투명성과 관련된 정보를 비치하여야 한다.

③ 선박보안경보시스템(제6규칙)

선박의 해상보안이 위협당할 경우 가까운 연안국 등에 도움을 요청하기 위한 선박보안경보시스템(Ship Security Alert System)을 도입하기로 하였다.

2004년 7월 1일 이후에 건조되는 모든 선박은 이 시스템을 설치하여야 하며, 2004년 7월 1일 전에 건조된 선박은 다시 2가지로 구분하고 있다. 즉, 총톤수 500톤 이상의 유조선, 케미컬 탱크, 가스운반선, 살물선 및 화물고속선은 2004년 7월 1일 후에 도래하는 첫 번째 무선설비검사 이전까지, 그리고 총톤수 500톤 이상의 기타 화물선 및 이동식 해양구조물은 2006년 7월 1일 후에 도래하는 첫 번째 무선설비검사 이전까지 설치하여야 한다.

④ 체약국 의무와 선장의 재량권(제7규칙 및 제8규칙)

체약국에게 영해에 운항하는 선박에 대한 보안수준 설정, 보안수준에 관한 정보 및 관련보안당국의 연락처 제공 등 의무를 부과하고, 선장에게는 선박안전과 보안이 상충될 경우 안전유지를 위한 조치를 취할 재량권을 부여하고 있다.

⑤ 통제와 이행조치(제9규칙)

타 체약국의 항만에 입항하려는 선박은 항만국 통제를 받아야 한다. 항만국 통제관은 입항선박에게 선박의 보안과 관련한 정보제공을 요구할 수 있다. 통제관은 선박이 관련 규정을 위반할 경우 선박의 지체 및 선박 억류, 항만내 이동을 포함한 운항제한, 추방 등의 조치가 가능하다. 단 위반선박에 대한 규제를 한 후에는 증서 발행조직과 국제해사기구에 통보하여야 한다.

⑥ 항만시설 요건(제10규칙)

체약국은 항만시설이 준수할 요건을 규정하고, 항만보안평가를 수행·검

토 · 승인하고, 항만보안계획서를 개발 · 검토 · 승인 및 이행하여야 한다.

2) ISPS Code

(1) 구성

ISPS Code는 Part A와 Part B로 구분되어 있으며, Part A는 이행이 강제되는 사항을, Part B는 임의규정으로 구성되어 있다.

(2) 적용(제3조)

국제항해에 종사하는 각 선박에 대하여 적용한다. 즉, 고속 여객선을 포함한 여객선, 고속 화물선을 포함한 총톤수 500톤 이상의 화물선, 이동식 해양구조물 및 국제항해에 종사하는 선박과 관련된 항만시설이 적용대상이다. 그러나 관공선, 군함, 비상업용 목적의 정부소유 선박은 적용이 제외된다.

(3) 당사국 정부의 책임(제4조)

당사국 정부의 책임은 보안등급 설정 및 보안선언, 보안관계 연락처 선정 및 관련 선박에 제공, 항만내의 선박 또는 입항하려는 선박에 대한 통제, 항만시설 보안평가, 보안계획서 승인, 선박보안계획서 승인 및 선박보안심사, IMO에 필요사항 통보, 타 당사국과 상호 보안협정문 체결(필요시) 등이다.

(4) 선박과 관련한 규정

① 보안선언서(제5조)

선장 또는 선박을 대신하는 선박보안책임자가 보안선언서(Declaration of security)를 제출하여야 하는 경우는 i) 인터페이스하고 있는 항만시설 또는 다른 선박보다 상위의 보안등급으로 선박이 운항하고 있는 경우, ii) 국제항로 또는 이들 항로를 운항하는 특정선박에게 적용하는 보안선언서에 관한 당사국

정부간 협정이 있는 경우, iii) 적용 가능한 선박 또는 항만시설에 영향을 미치는 보안위협 또는 보안사건이 있었던 경우, iv) 승인된 항만시설보안계획서의 소지 및 시행이 요구되지 아니하는 항만에 선박이 있는 경우, v) 승인된 선박 보안계획서의 소지 및 시행이 요구되지 아니하는 다른 선박과 선박 대 선박활동을 수행하는 경우이다.

② 회사의 의무(제6조)

선박보안계획서에 선장의 권한을 강조하고 정부 및 회사에 지원을 요청할 최우선의 책임 및 권한을 가짐을 명시하여야 한다.

③ 선박보안(제7조)

선박은 당사국 정부가 설정한 보안등급(Security Level - 등급 1/2/3) 별 적절한 조치를 수행하여야 한다.

④ 선박보안평가(제8조)

선박보안평가(Ship Security Assessment)는 전문가에 의해 수행되어야 한다. 선박보안평가는 현장검사를 포함하고 문서화하여야 한다. 선박보안평가에 포함될 주요내용은 시행 중인 보안조치, 절차 및 활동에 대한 식별, 중요하게 보호되어야 하는 주요 선상작업의 식별 및 평가, 보안조치의 수립 및 우선순위를 선별하기 위한 주요 선상작업에서 발생할 수 있는 위협 및 발생가능성의 식별 및 평가, 기반시설, 정책 및 절차에 있어서 인적요소를 포함한 취약성의 식별 등이다.

⑤ 선박보안계획서(제9조)

각 선박은 주관청에 의해 승인된 선박보안계획서(Ship Security Plan, SSP)를 선내에 비치하여야 한다. 선박보안계획서는 보안인증심사 대행기관(Recognized Security Organization, RSO)이 작성할 수 있다. 주관청은 선박보안계획서의

검토 및 승인업무를 보안인증심사 대행기관에 위임할 수 있다. 선박보안계획서는 비인가자의 접근 및 폭로로부터 보호되어야 한다. 선박보안계획서는 계약당사국 정부의 검사를 받지 않았거나, 부적합사항과 관련한 명백한 근거가 있는 경우, 선장 또는 선박의 동의가 있을 경우 열람이 가능하다. 그러나 선박보안계획서 중 일부 비밀정보로 취급되는 부분은 당사국 정부의 동의가 필요하다.

⑥ 기록(제10조)

선박보안계획서에 등재된 활동의 기록을 일정기간 동안 선내에 보유하여야 한다. 기록은 사용언어로 작성·보관하되, 영어, 불어 또는 스페인어 중 하나로 번역하여야 한다.

⑦ 회사보안책임자(제11조)/선박보안책임자(제12조)

회사는 회사보안책임자(Company Security Officer, CSO)를 임명하여야 한다. 복수의 회사보안책임자를 지정할 수 있다. 선박보안책임자(Ship Security Officer, SSO)는 선박단위로 임명하여야 한다.

⑧ 선박보안의 교육, 훈련 및 연습(제13조)

회사보안책임자와 관련 육상근무자 및 선박보안책임자는 보안과 관련한 지식 보유 및 훈련을 이수하여야 한다. 특정 보안업무 및 책임이 있는 선상근무자는 보안관련 임무수행에 필요한 지식과 능력을 보유하여야 한다. 선박보안계획서에 따라 적절한 간격으로 훈련을 실시하고 회사보안책임자는 연습에 참여하여야 한다.

⑨ 선박의 심사 및 증서발급(제19조)

선박이 받아야 할 심사의 종류는 최초심사, 갱신심사(5년), 최소 한번 이상의 중간심사, 주관청이 결정한 추가검사 등이 있다. 선박심사는 주관청 관리가

실시하나 보안인증심사대행기관에 위임이 가능하다. 초/갱신심사 후 국제선박 보안증서(International Ship Security Certificate, ISSC)가 발행된다.

(5) 항만시설과 관련한 규정

① 항만시설보안(제14조)

영해내 항만시설은 당사국 정부가 설정한 보안등급(Security level)에 따라 행동하여야 한다. 체약국은 항만시설보안으로 인한 승객, 선박근무자, 방문객의 간섭과 화물과 서비스 지연의 최소화에 노력하여야 한다. 이 조에서는 보안등급 1, 2, 3별 항만시설이 조치하여야 할 사항 또는 특정보호조치를 요구하고 있으며, 항만시설보안책임자와 선박보안책임자간의 상호교신 및 담당기관에 보고사항도 규정하고 있다.

② 항만시설보안평가(제15조)

항만시설보안평가(Port facility security assessment)는 당사국 정부가 수행한다. 특정 항만시설보안평가를 보안인증심사대행기관에 위임하는 것은 가능하다. 보안평가의 적합성 검토 및 승인은 당사국 정부가 직접 수행하여야 한다. 항만시설보안평가 수행자는 적절한 기술을 보유하여야 한다. 항만시설보안평가에 포함될 주요 내용은 중요하게 보호되어야 하는 주요자산 및 기반시설, 보안조치의 우선순위를 정하기 위한 자산 및 기반시설에 대한 예상위협 및 발생 가능성, 보안취약성 및 취약성을 감소시키기 위한 대응방안, 기반시설, 정책 및 절차에 있어서, 인적요소를 포함한 약점의 식별 등이다.

③ 항만시설보안계획서(제16조)

각 항만시설은 보안평가를 근거로 당사국 정부가 승인한 항만시설보안계획서(Port Facility Security Plan, PFSP)를 개발하고 유지하여야 한다. 당사국 정부의 승인을 조건으로 보안심사대행기관이 항만시설보안계획서를 작성할 수

있다.

항만시설보안계획서는 항만의 보안계획 또는 기타 항만비상계획과 통합 또는 일부분으로 구성할 수 있다. 당사국 정부로부터 항만시설보안계획서의 개정 승인없이 보안계획의 변경 및 시행할 수 없고, 항만시설보안계획서는 무단접근 및 폭로로부터 보호되어야 한다. 항만시설의 설계가 유사하다면 다수의 항만시설에 대해 하나의 항만시설보안계획서를 작성할 수 있다.

④ 항만시설보안책임자(제17조)

각 항만시설단위로 항만시설보안책임자(Port Facility Security Officer, PFSO)가 지정되나, 하나 이상의 항만시설에 대해 한 명의 항만시설보안책임자도 지정가능하다. 이 조에서는 항만시설보안검사, 항만시설보안계획서 개발·유지·시행 등을 포함한 항만시설보안책임자의 의무와 책임을 규정하고 있다.

⑤ 항만시설보안에 관한 교육, 훈련 및 연습(제18조)

항만시설보안책임자와 관련 항만시설보안요원은 보안과 관련한 지식을 보유하고 훈련을 이수하여야 한다. 특정 보안업무를 담당하는 항만시설근무자는 보안관련 임무수행에 필요한 지식과 능력을 보유하여야 한다. 적절한 간격으로 항만시설보안에 관한 훈련실시하고, 항만시설보안책임자는 훈련 및 연습에 참여하여야 한다.

3) 해상불법행위억지협약

(1) 1988년 SUA 협약 및 의정서

① 개요

‘항해의 안전에 대한 불법행위의 억제를 위한 협약(이하 ‘1988년 SUA 협약

약'이라 함)²⁴⁾은 항해중인 선박의 안전을 위협하는 선박 납치 등 해상테러를 규제하기 위하여 IMO가 1988년 이탈리아 로마에서 채택한 협약이다.²⁵⁾ 1998년 SUA협약의 채택 목적은 i) 항행의 안전에 대한 모든 불법적인 행위의 예방, 그 범죄자들의 기소 및 처벌을 위한 조치를 효과적이고 실제적 취하기 위한 국가간의 협력강화이다. 1998년 SUA 협약의 적용대상을 동력선, 잠수함 또는 기타 부양선을 포함하여 영구적으로 부착되지 아니한 모든 형태의 선박이다. 한편 IMO는 1998년 SUA협약의 적용대상에서 제외되어 있는 대륙붕에 위치한 고정구조물의 안전에 대한 불법적 행위의 억제를 위하여 '대륙붕에 설치한 고정 해상 플랫폼의 안전에 대한 불법행위 억제에 관한 1988년 의정서'(이하 '1988년 SUA 의정서'라 함)를 1998년 SUA협약과 함께 채택하였다. 1998년 SUA협약 및 동 협약의정서는 1992년 3월 1일 발효되어 2005년말 현재 G-7, 중국, 러시아 등 50여 개국이 가입된 협약이다. 주요내용은 운항중인 선박과 대륙붕상 고정된 플랫폼에 대한 불법행위에 대해 범죄인 인도, 관할권, 처벌조항 등을 규정하고 있다. 우리나라는 2003년 5월 27일에 「선박및해상구조물에대한위해행위의처벌등에관한법률(법률 제06880호)」을 제정하여 1988년 SUA협약 및 의정서를 국내법으로 수용하였다. 아울러 2003년 5월 14일 및 6월 10일 각각 1998년 SUA협약(조약 제1645호) 및 의정서(조약 제1648호)를 IMO 사무총장에게 가입서를 기탁함으로써 동 협약은 각각 2003년 8월 12일 및 2003년 9월 8일자로 우리나라에 발효하였다.

② 주요 내용

가. 적용범위

선박이 한 국가의 영해의 바깥한계 또는 인접국에 대한 동 국가의 영해의

24) 이 협약의 정식명칭은 “Convention for the suppression of unlawful acts against the safety of maritime navigation”임. 1988년 3월 10에 제정되어 4년이 지난 1992년 3월 1일에 국제적으로 발효되었으며, 2005년 12월 말 현재 126개국이 비준하였음. 협약에 가입한 국가의 선박량은 세계 상선대의 82.11%를 차지하고 있음.

25) 본래 SUA 협약을 제정한 것은 1985년에 일어난 이탈리아 여객선 아킬레 라우로 호 납치 사고로 미국인 여객이 피살된 것을 계기로 국제적인 대응방안을 마련하기 위한 것이었음.

횡적한계의 밖에 위치한 수역안으로, 동 수역을 통과하여, 또는 동 수역으로부터 항해중이거나 항해할 예정인 경우에 적용된다. 즉, 선박이 공해로부터 특정 국가의 영해로 진입하거나 특정국가의 영해로부터 공해로 항해중인 경우와 공해를 항해중인 때에도 적용된다. 그리고 협약이 이 규정에 따라 적용되지 아니한 경우에도 범죄자 또는 범죄혐의자가 상기 국가 이외의 당사국의 영토에서 발견될 때에도 적용된다.

나. 범죄구성 요건

SUA협약은 불법적 또는 고의적으로 무력 또는 협박에 의해 i) 선박을 납치 또는 점거하는 행위 ii) 선박의 안전운항을 위협에 빠뜨릴 가능성이 있는 선박 탑승자에 대한 폭력행위, 선박파괴행위, 선박이나 화물훼손행위, iii) 선박 파괴 또는 선박이나 화물의 훼손 가능성이 있는 물건을 그 선박 또는 해상구조물에 설치하거나 탑재하는 행위, iv) 선박의 안전을 위협하게 할 목적으로 그 선박 운항과 관련된 기기·시설을 파괴하거나 중대한 손상을 가하거나 기능장애상태를 야기하는 행위, v) 항해시설의 파괴·손상행위 또는 허위정보를 교환하는 행위, vi) 앞에서 규정한 모든 범죄행위 또는 그 미수와 관련하여 사람을 상해하거나 살해하는 행위를 하는 것을 범죄로 규정하고 있다. 그리고 이러한 범죄의 미수행위, 공범행위, 교사행위 및 위협행위도 범죄로 규정하고 있다(협약 제3조).

다. 재판관할권

SUA협약은 적용대상을 영해, 군도수역, 해협, 배타적 경제수역, 그리고 내수에서 일어난 테러행위에도 영향을 미친다. 먼저 각 당사국은 자국의 선박 및 영토에서 발생한 범죄와 자국의 국민에 의해 발생한 범죄에 대해 관할권을 가진다. 이에 추가하여 각 당사국은 자국이 통상적인 거주지인 무국적자에 의해 발생된 범죄, 범죄행위시 자국민의 납치·위협·상해 또는 살해된 경우나 자국에 대해 작위나 부작위를 강요하기 위하여 범죄가 행해진 경우는 해당국에

서 관할권을 확립할 수 있다. 이 경우는 각 당사국이 관할권을 확립한 때 또는 설정 후 포기한 때에는 IMO 사무총자에게 통지하여야 한다.

라. 범죄의 처리

각 당사국은 범죄자 또는 범죄 혐의자가 자국 영토 내에 체재하고 있는 경우는 자국법에 의해 범죄인에 대한 형사절차 또는 인도절차를 취하기 위한 범죄인의 구금 또는 신병확보 등 조치와 사실에 대한 예비조사를 즉시 취해야 한다. 그 경우 범죄자에 대한 형사관할권이 있는 당사국과 관련 이해당사국에게 범죄자의 구금과 그 정당성을 즉시 통보하여야 한다(협약 제10조제1항).

③ 1988년 SUA 협약 의정서의 주요내용

이 의정서는 SUA협약의 범위에서 제외되어 있는 대륙붕에 위치한 고정물에 적용하기 위하여 1998년 3월 10일에 SUA협약에 이어 채택된 것이다. 따라서 의정서의 내용은 1988년 SUA협약과 유사하다. 다만 이 의정서가 대륙붕에 위치한 고정 구조물에 적용되는 특성상 1988년 SUA협약에서는 범죄요건으로 규정하고 있는 i) 선박의 안전을 위협하게 할 목적으로 그 선박 운항과 관련된 기기·시설을 파괴하거나 중대한 손상을 가하거나 기능장애상태를 야기하는 경우, ii) 허위의 정보를 전달하여 선박의 안전운항을 위협하게 하는 경우 등은 적용이 없다는 점과 발효요건을 3개국을 정하고 있다는 점만 차이가 있다.

(2) 2005년 SUA 협약

① 협약 제정 배경

IMO는 2005년 10월 14일에 1988년 SUA 협약과 1988년 SUA 의정서를 개정하였다. 개정협약(이하 ‘2005년 SUA 협약’이라 함)을 제정한 것은 앞에서

언급한 바와 같이 2001년 9·11 테러 이후 국제적인 차원에서 테러를 예방하고, 테러행위를 자행한 범죄인에 대한 적절한 처벌규정을 마련하기 위한 것이다. 특히 IMO는 해사문제를 전담하는 유엔 산하 전문기구이므로, 선박의 운항과 관련하여 일어날 수 있는 해사 테러리즘을 규제하고 규율하는 방안의 하나로 기존의 1988년 SUA 협약을 전면적으로 개정, 2005년 SUA 협약을 다시 탄생시켰다. ISPS Code가 해사 테러리즘을 예방하는 데 초점을 둔 협약인 데 비해, 2005년 SUA 협약은 테러행위를 자행한 범죄인을 어떻게 처벌할 것인가 하는 점에 목적을 둔, 절차적 성격이 강한 국제협약이다.²⁶⁾ 이 개정협약에서도 9·11 테러 이후에 국제적인 보안 강화조치를 주도하고 있는 미국의 견해가 반영되었다. 예컨대 협약에 규정된 범죄 혐의가 있는 선박(의아 선박)에 대해 협약의 타방 당사국이 일방 당사국에 대해 승선 검색을 요청할 수 있는 조항 등이 그러하다.

특히 2005년 SUA 협약은 대량 살상 무기(WMD)²⁷⁾와 관련 물자 등이 선박으로 운송되는 것을 차단하기 위해 여러 가지 법적 장치를 두고 있는 것이 특징이다. 제2조에 WMD에 해당되는 무기와 물자 등에 대한 규정을 두고 있고, 제3조의 2와 3에서 1) 선박을 테러 수단으로 사용하거나 2) WMD를 운송하는 행위, 3) 협약에 규정된 범죄인을 선박으로 도피시키는 것을 모두 범죄행위로 규정하고 있는 것도 기존의 협약과 크게 다른 부분이다.

한편, 2005년 SUA 협약은 전문을 포함, 모두 24개 조문으로 구성되어 있는데, 제17조 이하의 협약의 가입과 비준, 그리고 발효 요건 등을 규정한 절차규정이다. 그런데 여기서 한 가지 유의해야 하는 점은 2005년 SUA 협약과 1988년 SUA 협약이 단일 문서로 통합되었다는 점이다. 따라서 2005년 SUA 협약에 가입한 국가들 사이에서는 두 협약이 하나의 협약 문서로 해석되고, 적용된다.²⁸⁾

26) 2005년 SUA 협약에서 해사 테러리즘 예방과 관련하여 둔 규정은 1988년 협약과 마찬가지로 제13조 1개 조문에 지나지 않으나 간접적으로 불법행위를 억제할 수 있는 몇 가지 조문을 두었음.

27) 협약에서 대량 살상 무기라는 용어는 직접 사용하지 않고 있으나 규정된 협약의 내용이 이와 관련되어 있어 논의 편의상 이와 같이 정리하였음.

28) 2005년 SUA 협약 제15조(해석 및 적용)

〈표 3-2〉 2005년 SUA 협약의 주요 내용

조 문	주요 내용	비고
제1조	2005년 의정서 목적상 협약, 기구, 사무총장 용어 정의 규정	해당 조문 신설
제2조	협약에서 사용되는 용어 정의. 운송 및 중대한 상해 또는 피해, BCN 무기, 독성화학물질, 원료 물질 등에 대한 정의 규정	선박을 제외한 WMD 관련 용어 규정 신설
제3조	기존 제2조에 1개 조문 추가 : 이 협약 시행이 다른 국제법(협약) 시행에 영향을 미치지 않음	제2조의 2 규정 신설
제4조	기존 3조에 3개 조문 추가 : 위해 목적으로 선박에 WMD·유류 등을 사용하거나 배출, 운송하는 행위, 선박을 피해발생수단으로 악용하는 행위, 범죤인을 선박에 승선시키는 행위 등을 범죄행위로 규정	범죄행위에 대한 규정 대폭 신설
제5조	기존 제5조에 1개 조문 추가 : 범인이 협약에 명시된 범죄행위를 한 경우 당사국에 대해 재정적 제재를 포함한 처벌의무 부과	제5조의 2 규정 신설
제6조	협약에 규정된 범죄에 대한 관할권 확정과 범죤인 인도 유무를 불문하고 IMO 통보에 관한 사항 규정	일부 규정 개정
제7조	협약의 부속서로 1970년 항공기 불법납치 억제협약 등 9개 협약을 추가. 이 부속서는 협약 비준시 적용을 배제할 수 있음	해당 조문 신설
제8조	당사국(선적국) 선박 선장은 범죄 혐의자를 타방 당사국(인수국)에 인도할 수 있음. 범죄를 억제하는데 필요한 당사국의 협조(사법공조) 및 승선·검색에 관한 규정 및 보호 조치 규정 신설	제8조의 2 신설
제9조	당사국 영토 안에 있는 범죤인에 대한 신속한 처벌과 공정한 대우 규정	일부 조항 개정
제10조	협약 범죄는 기존의 범죤인 인도 조약의 인도대상 범죄로 봄. 협약 범죄는 정치범죄로 인정하지 않음. 특별한 사정이 있는 경우 당사국은 범죤인 인도 거절 가능	일부 조항 개정 및 2개 조문 신설
제11조	협약에 규정된 범죄를 처벌하는데 필요한 증거 획득 등 형사소송절차에 대해 당사국 협력 필요	일부 조항 개정 및 1개 조문 신설
제12조	당사국은 협약에 정한 범죄를 예방하는데 필요한 협력을 해야 하며, 범죄 실행에 따른 피해 최소화에 노력함	일부 조문 개정
제13조	일방 당사국은 협약에 규정된 범죄 실행에 관한 정보를 입수한 경우 관할권 있는 다른 당사국에 제공함	조문 전면 대체
제14조	범죄 관련 정보와 범죤인 처벌상황 등을 IMO에 통보할 것	기존 협약 제15조 제3항 개정
제15조	1988년 SUA 협약과 2005년 개정의정서는 의정서 당사국 간에 단일 문서로 통합되고, 해석됨	해당 조문 신설
제16조	제17조 이하에 명시한 최종 규정이 2005년 SUA 협약의 최종 규정임을 명시	해당 조문 신설
제17조~제24조	협약의 서명, 비준과 발효요건, 개정 및 수정 등 절차 규정	해당 조문 신설

주 : 조문은 2005년 SUA 협약에 따른 것이며, 주요 내용은 1988년 SUA 협약과 통합된 조문임
 자료 : 2005년 SUA 협약에서 정리

② 협약 적용 범위의 확대

2005년 SUA 협약의 가장 큰 특징은 기존 협약에 비해 적용대상이 되는 범죄의 유형이 크게 늘어난 점이다. 기존 협약 제1조 정의 규정에서 선박에 대한 정의만 남겨 두고, 중대한 상해 및 피해, BCN 무기²⁹⁾ 등에 대한 규정을 둔 다음, 제3조를 개정하여 적용되는 범죄의 종류를 다양화하였다. 즉, 범죄의 유형을 정한 기존 협약 제3조 제1항을 수정하여 존치한 다음,³⁰⁾ 제3조 2와 3, 그리고 4를 차례로 신설하였다. 여기에서 특이한 것은 선박 자체를 테러 수단으로 사용하는 경우도 범죄행위로 규정하고 있는 점이다.

가. 제3조의 2 : 대량 살상 무기의 사용과 운송 관련 범죄

불법적 또는 고의적으로 아래에 명시한 행위를 하거나, 일정한 행위를 정부나 국제기구로 하여금 행하거나 행하지 않도록 강요하는 것을 범죄행위로 규정하였다.

(i) 사망하거나 중대한 상해 또는 피해를 발생하거나 발생하기 쉬운 수단으로 어떠한 폭발물질, 방사능물질 또는 BCN 무기를 선박에 대하여 또는 선상에서 사용하거나 선박으로부터 배출하는 행위, 또는

(ii) 상기 (i)에 해당되지 않는 기름, 액화천연가스 또는 기타 유해·유독 물질을 사망하거나 중대한 상해 또는 피해를 발생하거나 발생하기 쉬운 정도의 양 또는 농도로 선박으로부터 배출하는 행위, 또는

(iii) 사망하거나 중대한 상해 또는 피해를 발생하는 수단으로 선박을 사용하는 행위, 또는

(iv) 상기 (i)호, (ii)호 또는 (iii)호에 규정된 범죄를 범하기 위해 협박하는 행위 등이다.

29) BCN은 Biological, Chemical, Nuclear Materials를 의미함.

30) 1988년 SUA 협약에 규정되어 있는 범죄로는, 선박에 있는 사람에 대한 폭행, 협박, 상해, 살인죄와 선박 납치죄, 선박 손괴죄, 선박 운항관련 기기 및 시설의 손괴죄, 선박에 대한 위험 물건 설치 및 탑재죄, 선박의 안전을 해할 목적의 허위정보 전달죄, 선박 납치 살인, 치사죄 상해·치상죄 등을 규정하고 있음.

또한 폭발물질이나 원자력 물질, BCN 무기와 이 같은 무기의 제작에 관련된 장비, 물질 또는 소프트웨어 등, 그리고 국제원자력기구(IAEA)에서 보호받지 않는 핵관련 물질이나 장비 등을 선박에 운송하는 행위 등도 새로운 협약에서는 범죄에 해당한다.

나. 제3조의 3 : 범죄인을 선박으로 탈출·도피 방조 행위

이 협약은 또한 제3조 내지 제3조 4에서 규정한 범죄와 부속서에 수록된 9개 협약에 명시된 범죄를 구성하는 행위를 한 자를 인지하고, 형사 소추를 피하기 위해 선박에 승선시켜 도피시키는 행위도 범죄로 규정하고 있다.

다. 제3조의 4 : 협약에 정한 범죄의 음모, 교사, 방조죄

이 뿐만 아니라 2005년 SUA 협약은 제3조 내지 제3조의 3에서 규정한 일정한 범죄행위와 관련해 타인을 살해 또는 상해하거나, 교사와 방조죄에 대해서도 처벌하도록 규정하고 있다. 특히 이 협약은 상기한 범죄를 인지한 경우에도 처벌할 수 있는 길을 열어 놓고 있다.

③ 범죄 예방을 위한 협력

2005년 SUA 협약에서 범죄 예방과 관련해 둔 직접적인 규정은 제13조(개정정의정서 제12조)와 제8조의 2이다. 즉, 제13조는 기존의 조항을 그대로 둔 것이며, 후자는 특히 다른 당사국의 혐의 선박에 대한 승선 검색 요청과 관련되어 있는 규정이다.

첫째, i) 협약 당사국은 장소를 불문하고, 범죄를 실행할 목적으로 자국 영역 안에서 행해지는 준비활동을 방지하기 위한 모든 실행 가능한 조치의 실행과 ii) 국내법에 따른 정보의 교환, 협약에 규정된 범죄의 실행을 방지하기 위하여 취해진 적절한 행정조치, 기타 조치의 조정 등에 관한 사항을 중심으로 다른 당사국과 협력하여 범죄 예방에 노력하여야 한다.

둘째, 협약 당사국은 이 협약에 적용되는 불법행위를 방지·억제하기 위하

여 국제법에 의거, 가능한 범위 내에서 협력하여야 하며, 다른 당사국이 이 협약에 따라 범죄 예방에 필요한 정보를 요구하는 경우 이에 응해야 한다. 특히 이와 관련해 협약 당사국들은 혐의 선박의 선명, IMO 선박식별번호, 선적항, 출항항 및 목적항, 그리고 기타 모든 관련 정보를 제공할 수 있어야 한다.

셋째, 이번 협약에서는 협약 당사국에 설립된 법인에 대한 책임을 강화해 범죄를 차단하는 방안도 마련해 놓고 있다. 협약 제5조의 2로 신설된, 범죄 행위와 관련된 법인의 책임에 관한 규정이 그것이다. 즉, 협약에 따르면, 당사국의 국내법에 따라 설립된 법인을 관리·감독할 책임이 있는 자가 협약에 규정되어 있는 범죄를 행하는 경우에는 그 법인에 대해 민·형사 책임뿐만 아니라 행정적 책임까지 물을 수 있도록 명시되어 있다. 특히 협약은 법인에 대해 책임을 부과하는 경우 반드시 재정적인 제재를 포함하도록 함으로써 금전적으로 압박을 가할 수 있게 하고 있다.

④ 범죄 관련 정보의 통보

2005년 SUA 협약은 또한 당사국에 대해 범죄와 관련되어 있는 정보를 다른 당사국이나 국제해사기구(IMO)에 통보할 것을 의무화하고 있다.

첫째, IMO에 대해서는 제6조에 관할권 확정과 포기에 관한 사항, 협약 제8조의 2 제15항에 규정된 협약 시행에 필요한 관할 당국의 연락처, 당사국에 대해 협약이 발효하기 전에 정선 및 승선 검색권을 위임한 경우, 협약 제15조에 규정된 범죄의 상황, 범죄 예방과 관련하여 당사국 간에 협력한 사항, 범죄인의 처벌 결과 등을 IMO 사무총장에게 통보하도록 명시하고 있다. IMO 사무총장은 협약 당사국에서 접수한 정보를 회원국이나 적절한 정부간 기구에 통보할 수 있다.

둘째, 다른 당사국에 제공해야 하는 정보로는, 범죄인의 인도와 인수 등과 관련해 부대되는 정보, 다른 당사국이 요청한 혐의 선박의 선명이나 선적 정보에 관한 사항, 다른 당사국에 인도한 범죄인의 혐의 사실과 범죄를 입증할 만한 자료 등이 이에 해당된다.

⑤ 선박의 승선·검색 요청

2005년 SUA 협약의 백미는 WMD와 관련물자를 운송하는 혐의가 있는 선박에 대한 정선 및 승선 검색권이다. 협약에 신설된 제8조의 2에 이와 관한 사항이 주로 명시되어 있다. 즉, 일방 당사국의 관할 당국이 영해 밖에서 타방 당사국의 혐의 선박³¹⁾에 대해 승선 검색을 할 수 있는 길을 터놓고 있다. 이 경우 혐의 선박을 발견한 협약 당사국은 다른 당사국(선적국)에 대해 그 선박의 국적 확인을 요청할 수 있는데, 국적이 확인되면, 본격적으로 그 선박을 검색하기 위한 절차에 돌입하게 된다. 이 같은 절차를 표시하면 다음과 같다.

① 영해 밖에서 혐의 선박의 발견 → ② 선적국에 대해 선박국적 확인 요청 → ③ 선적국의 선박 국적 확인 → ④ 혐의 선박 발견 국가(요청국)가 선적국에 대해 승선 검색에³²⁾ 관한 권한 위임 요청 → ⑤ 혐의 선박 선적국의 대응 조치 등으로 이루어진다.

이 같은 요청을 받은 혐의 선박의 선적국은 ① 요청국에 대해 자국의 혐의 선박 검색권 위임, ② 자체적으로 승선 검색 실시, ③ 요청국과 공동으로 승선 검색 실시, ④ 요청국의 승선 검색 요청 거절 등 네 가지 조치를 할 수 있다.

그러나 이 같은 조치 가운데, 협약 당사국이 현실적으로 ④번 조치를 택할 가능성은 많지 않아 보인다. 협약 제8조의 2 제1항에 다른 국가에 대한 협조 의무를 규정하고 있을 뿐만 아니라 협약의 제정 목적이 해사 테러 등 해상에서 일어날 수 있는 불법행위를 막는 데 있기 때문이다.

한편, 요청국가에 대해 혐의 선박에 대한 승선 검색권을 위임한 것과 관계없이 선적국은 검색과정에서 압류, 몰수, 체포 및 기소 등을 포함한 억류된 선박, 화물 또는 기타 목록 및 승선중인 자에 대한 관할권 행사할 수 있다. 이와 반대로 요청국도 검색과정에서 협약에 규정된 범죄 사실을 입증할만한 증거를

31) 여기서 혐의 선박이라 함은 다른 제약국의 선박 또는 선박에 승선하고 있는 자가 협약 제3조, 제3조의 2, 제3조의 3 또는 제3조의 4 하의 범죄를 저질렀거나 가담하려고 하는 의심할 만한 합리적인 근거를 가지고 있는 경우를 말함.

32) 승선 검색에는 협약에 규정된 범죄 사실을 확인하기 위한 혐의 선박에 대한 정선과 선박에 적재되어 있는 화물, 승선중인 사람에 대한 질문과 검색 등이 포함됨.

발견한 경우 해당선박이나 화물 및 승선하고 있는 혐의자 등을 억류할 수 있는 권한을 위임해 줄 것을 선적국에 요청할 수 있다.

그리고 이 같은 승선 검색을 실시하는 협약 당사국에 대해서는 일정한 의무가 부과된다. 즉, 검색과정에서는 무력사용을 최소화해야 하며, 해상에서 인명을 보호하는데 필요한 적절한 조치를 강구해야 하는 한편, 선박과 화물의 안전 및 보안을 고려해야 하는 등 여러 가지 세이프 가드를 이행해야 한다. 또한 이 같은 승선 검색으로 인해 부당하게 피해를 입은 경우 협약 당사국은 손해를 배상할 책임이 있다(협약 제8조의 2의 제(b)항)).

〈표 3-3〉 범죄혐의선박에 대한 승선·검색 절차

구분	승선·검색 절차
기국의 동의절차에 따른 승선·검색	- 요청국이 범죄혐의선박의 기국에게 국적확인 통지 및 확인 - 승선·검색 권한 위임요청 - 기국의 결정에 따른 조치 수행 · 기국이 요청국에게 승선 및 검색권 위임 · 기국이 직접승선·검색 실행 · 기국이 요청국과 공동으로 승선·검색 실행 · 기국이 요청국의 승선·검색요청 거절
묵시적 임의승선·검색 동의	- 동의방법 : 개정의정서 비준·가입시 또는 그 후 사무총장에 대한 통지 - 동의조건 : 요청국이 범죄혐의선박에 대해 기국에 국적확인을 통지하였으나 4시간 이내 무응답일 경우 - 동의내용 : 요청국은 임의승선·검색
사전허용에 의한 승선·검색	- 허용방법 : 개정의정서 비준·가입시 또는 그 후 사무총장에 대한 통지 - 허용내용 : 요청국은 범죄혐의선박이 있을 때 기국의 동의없이 승선·검색

⑥ 승선·검색결과 조치

혐의선박에 대한 승선·검색결과 협약 위반증거를 발견한 경우 기국은 승선 검색국에게 당해 선박·선원·화물의 억류를 허용할 수 있다. 승선검색국은 그 결과를 기국에 즉시 통보하여야 한다. 또한 승선검색 결과 이 협약의 적용

대상이 아닌 불법행위의 증거를 발견한 경우 그 결과를 기국에 즉시 통보하여야 한다. 승선검색과정에서 임무수행과 집행기관의 안전에 필요한 경우, 그리고 집행과정을 방해하는 경우에는 무력을 사용할 수 있다. 한편 협약은 범죄협 의 선박의 승선·검색과정에서 일반적 준수사항을 규정하고 있고, 강제승선·검색결과 무협의원 경우 취해진 조치로 인한 피해에 대한 승선검색국의 책임을 규정하고 있다(제10조(a) 및 (b)항).

⑦ 발효

개정 의정서는 2006년 2월 14일부터 1년간 서명을 위해 개방될 예정이고, 12개국 비준 후 3개월이 지나면 발효하게 된다.(플랫폼의정서는 3개국 비준으로 발효하지만 개정 의정서보다 앞서 발효하지 못하도록 함).

⑧ 부속서

개정 의정서는 부속서의 반테러협약의 범죄자를 도피방조한 운송행위를 범죄행위로 규정하고 있다. 개정협약에서 부속서로 두고 있는 협약은 다음과 같다.

- i 항공기의 불법납치억제를 위한 협약
- ii) 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약
- iii) 인질억류방지에 관한 국제협약
- iv) 핵물질의 방호에 관한 협약
- v) 제2항 협약에 보충하는 국제민간항공기가 이용하는 공항에서의 불법적 폭력행위의 억제를 위한 의정서
- vi) 대륙붕상에 고정된 플랫폼의 안전에 대한 불법적 행위의 억제를 위한 의정서
- vii) 폭탄테러행위의 억제를 위한 국제협약
- viii) 채택된 테러자금조달의 억제를 위한 국제협약

4) 시사점

국제해사기구(이하 해사기구)는 선박의 항로, 교통규칙, 항만시설 등을 국제적으로 통일하기 위하여 설치된 유엔 전문기구로 국제해운의 안전, 항행의 능률화와 각종 제한의 철폐를 위하여 해운 문제의 심의, 정보교환, 조약의 작성이나 권고를 임무로 하고 있다. 따라서 엄밀하게는 선박과 항만의 보안문제는 이 기구의 목적과 완전히 부합되지는 않는다. 그러나 9·11 테러에 이 기구에서 채택하거나 개정한 협약, 즉 ISPS Code나 2005년 SUA협약은 선박 및 항만에 대한 보안과 WMD 등을 차단하는데 초점을 맞추고 있다. 특히 2005년 SUA 협약의 제정은 미국을 중심으로 하는 국제사회가 선박이 테러의 목표가 되거나 테러의 수단으로 악용되는 점을 용납하지 않겠다는 강력한 의지를 밝힌 것이다. 이 협약 제정으로 IMO는 2001년 이후 논의돼온 해사 테러리즘과 관련된 대책을 모두 내놓은 셈이다.

그런데 2005년 SUA 협약의 상당 부문은 현재 미국 등 여러 나라가 도입한 PSI(Proliferation Security Initiative), 즉 대량살상무기 확산 방지 구상과 맞물려 있다. PSI는 미국 부시 대통령이 2003년 5월 폴란드를 방문하는 자리에서 발표한 미국의 대테러 외교 정책의 하나로, WMD와 관련 물자를 운송하는 혐의가 있는 항공기나 선박을 차단하는 것을 주요 내용으로 하고 있다.³³⁾ 특히 이 제도는 도입 초기부터 이른바 미국이 주장한 악의 축 또는 불량 국가로 지목된 북한과 이란 등을 겨냥한 것이 아니냐는 의혹 때문에 많은 논란을 빚어왔다. 그러나 PSI 제도를 도입한지 3년이 지난 지금, 가입국 수가 70여 개국으로 확대되고, 세부 행동 지침이 마련됨에 따라 구체적인 테러 차단 전략으로 자리를 잡고 있다.

또한 미국은 이번 2005년 SUA 협약 제정을 통해 불법 무기를 운송하는 혐의가 있는 선박에 대해 승선 검색할 수 있는 근거를 마련해 놓았다. 즉, 미국

33) 항공기의 경우 사실상 차단이 불가능하기 어렵기 때문에 이 제도는 주로 선박에 초점을 맞추고 있는 것이 사실임.

의 PSI가 국제 규범화하고 있는 셈이다. 우리나라는 새로운 협약에서 정하고 있는 혐의 선박에 대한 승선 검색권을 수용해야 하는 문제와 이 협약 수용으로 인해 남북관계에 있어 불필요한 오해를 불러 올 소지가 없는지 판단해야 할 시점에 와 있다. 협약 서명을 위해 개방되어 있는 2007년 2월 13일까지, 그리고 다른 국가의 비준 동향을 주시하면서 협약 가입 시기와 실익을 신중하게 판단할 필요가 있다.³⁴⁾

2. 국제관세기구(WCO)

세계세관기구(WCO)는 2005년 6월 27일 166개국 회원국 대표가 참석한 가운데 벨기에 브뤼셀 본부에서 회의를 개최하고, 그 동안 논의하던 ‘물류보안과 무역 간소화에 관한 국제 기준(일명, Framework)’을 정식으로 채택하였다.³⁵⁾ 이 기준은 현재 미국에서 도입하여 시행하고 있는 컨테이너 보안협정(CSI)과 반테러 민-관 파트너십 제도(C-TPAT)를 합친 것으로, 미국의 보안제도를 전 세계적으로 확산시키는 효과가 있는 것으로 판단되고 있다.

이 기준의 제정에 따라 각국의 세관 당국은 자국에 또는 자국으로 수출입 되는 화물에 대한 정보를 국제적으로 통일된 방식에 따라 사전에 전자적인 방법으로 신고를 받을 수 있게 되었으며, 화물을 수입하는 국가가 요청하는 경우에는 수출 화물에 대해 미리 항만에서 위험물 등의 적재여부를 검색해야 한다. 지금까지 미국과 공동으로 컨테이너 보안협정을 시행하는 국가에서는 미국으로 수출되는 컨테이너 화물에 대해서만 위험 화물의 적재 여부를 화물 검색기 등을 이용하여 검사해왔다.

2005년 7월 4일자 아메리칸 쉬퍼에 따르면, 이 기준이 제정된 이후 미주와

34) 미국은 최근 이 협약과 2005년 SUA 협약 의정서에 가입한 것으로 알려졌다(American Shipper, 2006. 2. 20).

35) 새로운 보안규칙의 명칭은 ‘WCO Framework of Standards to Secure and Facilitate Global Trade’임.

아시아, 오세아니아 등 98개 국가가 이를 조만간 시행할 계획이 있는 것으로 알려졌다. 유럽연합의 경우 25개 회원국이 단일서명형식으로 이 기준을 공동으로 시행한다고 밝힌 것을 비롯해 미국과 멕시코, 캐나다, 일본, 러시아, 호주 등 거의 100여 개 국가가 이 제도를 시행하기로 합의했다고 WCO의 관계자가 덧붙였다.³⁶⁾ 다음에서는 WCO의 Framework에 대해 검토한다.

1) WCO의 프레임워크

(1) 프레임워크 제정 목적

WCO가 프레임워크를 제정한 목적은 6가지로 요약될 수 있다. 첫째, 국제적인 수준에서 공급체인상의 보안 및 무역을 촉진하고 확실성 및 예측성을 보장하고자 국제표준을 마련하는 데 있다. 둘째, 모든 운송수단을 위한 통합 공급체인관리를 가능케 하는 데 있다. 셋째, 21세기의 도전과 기회들에 대한 관세의 역할, 기능, 그리고 능력을 향상시키는 데 있다. 넷째, 위험 수위가 높은 위탁화물을 검색하고 세관 능력을 향상하고자 각국의 세관들과 공조체제를 강화하는 데 있다. 다섯째, 세관과 기업의 협력체제를 강화하는 데 있다. 여섯째, 국제거래 공급체인의 보안 확보를 통한 막힘없는 화물의 이동을 증진하는 데 있다.

(2) 프레임 워크의 4가지 핵심 요소

WCO 프레임워크는 4가지 핵심요소로 구성되어 있다. 첫째, WCO 프레임워크는 수입, 수출, 그리고 환적 화물에 대한 진보된 전자적 화물정보 요구사항들과 조화를 이루고 있다. 둘째, WCO 프레임워크에 합의한 각 국가는 보안위협에 대해 일관된 위험관리 접근방법을 채택해야 한다. 셋째, WCO 프레임워크는 위험화물 관리 방법에 의한 수입국의 합당한 요구 사항에 대해 수출국의 세관은 위험 수위가 높은 수출 컨테이너나 화물에 대해서 비파괴검사 방법인 X-ray 장

36) *Americanshipper*, 2005년 6월 27 및 7월 4일자.

비나 방사선 감지기를 이용한 검사를 수행할 의무가 있다. 넷째, WCO 프레임워크는 기업이 공급망 보안에 대한 기준을 이행할 경우 누릴 수 있는 혜택에 관해서 규정하고 있다.

(3) 프레임워크의 2가지 기본 축

앞에서 언급한 WCO 프레임워크의 4가지 핵심 요소를 바탕으로 하여 WCO 프레임워크는 협의체 세관들 간의 협정(Customs-to-Customs Network Arrangements)과 세관과 기업들 간의 파트너십(Customs-to-Business Partnerships)이라는 2가지 기본 Pillar로 구성되어 있다. 이러한 2가지 기본 Pillar의 개념을 적용함으로써 다양한 이점을 창출할 수 있다. 기본 Pillar들은 협의체 간의 이해를 용이하게 하고 빠르게 국제적으로 이행되어 질 수 있도록 통합된 보안 표준들의 집합으로 구성되어 있다. 더욱이 이 프레임워크는 회원국들에 의해 개발된 기존의 WCO 보안 및 촉진에 관한 기준과 프로그램에 기초하고 있다.

(4) 프레임워크 시행 혜택 및 이점

WCO 프레임워크는 국제교역의 촉진, 테러에 대한 보안 유지 확대, 국가의 경제 및 사회적 복지에 대한 세관과 거래국간의 혜택을 향상시키는 등의 새로운 통합된 기초(platform)적인 역할을 제공한다.

① 국가/정부

WCO 프레임워크의 주요 목적 중의 하나는 테러에 대한 보안을 유지하여 국제 무역을 촉진하고자 하는 데 있다. 따라서 이 프레임워크는 국제적인 테러 위협에 대한 거래의 안전성을 확보하도록 도움을 줌으로써 세관들이 적법한 화물에 대한 이동을 촉진하고, 세관운영의 향상, 현대화하는 데 도움을 줄 것이다. 또한 수익 증진, 국제법과 규정의 적절한 응용에도 도움을 줄 것이다. 따라서 WCO 프레임워크는 경제 및 사회적 안정을 보장하고, 외국직접투자를 촉진하는 데도 도움을 줄 수 있다.

WCO 프레임워크는 세관과 다른 정부 기관들 간의 협력을 위해서 협정을 체결할 것을 권유한다. 더불어 협정 체결시 기존의 국제표준들을 확인할 필요가 있다. 따라서 정부로 하여금 통합된 국경관리 및 통제를 강화하는 데 도움을 줄 수 있고, WCO 프레임워크는 정부로 하여금 세관의 강제성과 책임을 확장하는 데 권한을 부여한다.

② 세관

WCO 프레임워크의 주요 신뢰성을 가지는 한 분야는 국제거래 공급망에서 보안을 확보하여 막힘없는 화물의 흐름을 증진하기 위해서 세관-세관간의 협정을 체결하는 것이다. 이러한 네트워크 간의 협정은 세관들 간의 협조체제를 구축함으로써 효과적으로 위험에 대처할 수 있도록 적시에 정확한 정보를 교환할 수 있게 한다. 즉, 국제거래 공급망에서 위험 높은 위탁화물에 대한 검색 능력을 증가시키고 효과적으로 세관 업무를 분할함으로써 세관통제를 강화하는 데 도움을 준다. 더불어 세관들 간에 체결한 이 협정은 불확실성한 환경에서 상호간의 통제에 대한 신뢰를 제공할 수 있다.

③ 기업

WCO 프레임워크는 국제거래에서 테러에 대한 보안을 확보하고 국제교역을 촉진하는 것을 목표로 하고 있다. 또한 이 프레임워크는 현대적인 글로벌 생산 및 분배 모델을 기본으로 하고 있다. WCO 프레임워크의 주요 구상 가운데 한 부분은 AEOs(Authorized Economic Operators) 자격을 얻는 국제표준에 관한 안을 포함하고 있다. AEOs란 WCO나 이에 상응한 공급관리 보안 표준안에 의거하여 국제적으로 합의된 자격을 취득한 국제적 화물운송에 참여한 단체를 일컫는다. AEO의 대상 업체는 글로벌 제조업체, 수입업자, 수출업자, 브로커, 항만, 공항, 터미널 운영업자, 창고업자, 물류업체 등을 포함한다. AEO의 자격을 갖춘 기관에게는 통관절차의 간소화 등의 혜택을 부여하고 전 세계 당국이 이 혜택을 인정한다는 것이다.

(5) 회원국 네트워크 강화

효과적인 네트워크 강화는 WCO 프레임워크를 광범위하게 적용하고 실행하게 하는 중요한 요소이다. 그러나 이 프레임워크의 일정 부분은 즉각적으로 실행 가능하게 되어 있다. 결과적으로 회원국들은 WCO 프레임워크를 이행할 수 있도록 네트워크 확대에 관한 전략을 준비해야 한다. 이러한 네트워크 확대를 성공적으로 수행하기 위해서는 정치적 의지와 통합이 우선시되어야 한다. 따라서 WCO 프레임워크와 정치적 의지를 수행하고자 하는 국가들은 WCO 및 회원국과 협력 파트너들의 지원을 받아야 한다.

(6) 프레임워크의 이행절차

WCO 프레임워크가 이행되기 위해서는 네트워크 확대뿐만 아니라 단계적인 접근방법에 대한 이해가 동반되어야 한다. 개별 국가 차원에서 즉각적으로 이행하고자 하는 것은 바람직하지 않다. 비록 WCO 프레임워크가 필요한 최소한의 표준으로 구성되어 있지만 개별 국가의 능력과 필요한 법적인 기관과 협조하여 다양한 수준에서 이행되어야 한다. 상위수준 전략그룹(High Level Strategic Group)과 협조하여 WCO 사무국은 프레임워크의 표준에 대한 이행 계획을 수립할 계획이다. 이 프레임워크는 먼저 프레임워크를 적용하고 실행 시 이점들을 기술한다. 둘째, 세관-세관 협의회 간의 협정들과 세관-기업들 간의 파트너십을 다루는 뼈대 구축, 그리고 마지막으로 세부 수행 지침을 포함한 부가사항 요소를 작성한다. 궁극적으로 이 프레임워크는 차후 더욱 개선, 보완될 것이며, 적용시 국가/정부, 세관, 기업들에게 다양한 이점을 제공할 것이다.

2) WCO의 프레임워크 표준안

(1) 세관-세관 Pillar(The Customs-Customs Pillar)

공급망의 보안 및 국제교역의 촉진을 극대화하고자 세관은 일반 및 협의된 표준안들에 대해 협조적으로 업무를 수행해야 한다. 세관-세관 Pillar는 이러한

목적을 달성하고자 하는 것이다. 즉, 테러 및 다국적 범죄에 대하여 공급망상의 국제거래의 보안을 확보하는 효과적인 메커니즘을 제공하고자 하는 것이다. 전통적으로 세관은 화물이나 컨테이너를 자국의 항만에 도착했을 때 검사를 수행한다. 그러나 현재에는 화물이 도착하기 전에 검사할 수 있는 능력이 요구된다.

세관-세관 Pillar에서 중요한 구성요소는 위험도가 높은 화물이나 컨테이너를 검색하기 위해 첨단전자정보를 활용하는 것이다. 자동화된 도구를 사용하여 세관은 선적 항만에서 출발하기 전에 위험도가 높은 화물을 확인한다. 정보를 자동적으로 교환하기 위한 대책이 준비되어야 한다. 따라서 이 시스템들은 표준화된 양식을 필요로 한다.

효과적이고 효율적인 화물의 운송을 위해 세관은 위험화물을 검사할 수 있는 최첨단 장비를 사용해야 한다. 대형 X-ray, Gamma-ray 장비, Radiation 장비 등이 그 예가 될 수 있다. 따라서 최첨단 검사 장비를 활용하는 것도 세관-세관 Pillar에서 중요한 요소 중의 하나이다. 개정 교토협약(Revised Kyoto Convention),³⁷⁾ 통합공급망관리(Integrated Supply Chain Management) 지침, 국제적 프로그램, WCO 프레임워크에 가입한 세관들은 Pillar 1을 표준화한다.

(2) Pillar 1 Standards(11개 기준)

① Standard 1 : 통합 공급망 관리(Integrated Supply Chain Management)
세관은 통합 공급망관리에 대한 WCO 관세 지침에 의거하여 통합 통관절차를 준수해야 한다.

가. 범위

통합된 관세 통제를 이행하기 위해 세관이 수출업자로부터 세관자료보안 위

37) 개정 교토협약은 통관절차의 표준화, 통관절차의 신속화 및 간소화, 정보기술의 최대 활용 등을 주요 원칙으로 국제협약 개정 의정서이다. 아직은 강제성을 가지지는 않지만 2005년 6월에 40개 협약 가입국 가운데 38개국이 1973년 교토협약의 수정안에 동의했다.

협평가를 목적으로 사전 전자정보를 요구할 수 있는 법적기관이 필요하다.

나. 일반 통제 조치

가) 세관통제

개정 교토협약은 관세영역을 출입하는 운송수단을 포함하여 모든 물품은 세관 통제의 대상으로 간주한다. 위탁화물의 무결성은 물품이 컨테이너에 적재되는 시점부터 목적지 세관통제가 해제될 때까지 보장되어야 한다. 또한 컨테이너에 적재할 수 없을 경우에는 운송 수단에 선적되는 시점부터 보장되어야 한다.

나) 위험 평가

보안을 목적으로 하는 세관통제와 위험평가는 수출업자가 물품을 준비하는 시점에서부터 불필요한 세관절차를 배제하고 화물의 무결성을 확인하고자 공급망의 전 통관절차에서 공통적으로 이행되어야 한다. 이를 위해서 세관은 WCO 글로벌 정보와 안보 전략(WCO Global Information and Intelligence Strategy)에 의거하여 화물의 위험 특징 자료 공유와 세관 데이터의 교환에 대해서 일괄적인 통제와 위험관리 표준을 준수해야 한다. 이러한 협정은 표준의 준수 여부를 확인하는 품질관리 절차도 고려해야 한다.

다) 출발지 통제

출발지 세관 사무소는 공급망에서 위탁화물의 확인과 불법적 방해요소를 검색할 수 있는 사용가능한 모든 조치를 취해야 한다. 해상화물의 경우 컨테이너에 적재되어 선박에 선적되기 전에 검사, 검역, 위험평가 등이 수행되어야 한다.

라) 봉인

공급망에서의 보안과 원활한 일련의 통관 프로세스를 확보하기 위해 세관은 개정 도쿄협약(Revised Kyoto Convention)에 수록된 일반부록 6장의 수정된

지침에 명시된 봉인무결성 프로그램을 시행해야 한다. ISO/PAS 17712에 제시된 첨단 보안기기를 사용해 잠금 시점에서 봉인 무결점 프로그램은 운송수단이 바뀌는 부문에서 봉인 상태를 점검하는 절차를 포함한다. 더불어 세관은 공급망에서 컨테이너의 무결점을 확보하기 위해 자발적으로 첨단 기술을 도입해야 한다.

마) 고유 화물 인식번호(Unique Consignment Reference)

세관은 고유화물 인식번호 부여할 때 WCO 권장 사항과 지침을 준수해야 한다.

다. 데이터 전송

가) 수출물품 신고(Export Goods Declaration)

화주 혹은 화주의 에이전트는 화물을 컨테이너에 적입하거나 운송수단에 직접 선적하기 전에 사전에 화물에 대한 정보를 수출지 세관에 전자적으로 수출 신고서를 제출해야 한다. 수출신고서에 필요한 기본적 정보는 화주, 운송대리인, 캐리어 번호, 수입업자, 화물인수인, 목적지, 경유국가, 에이전트, 관세코드, 위험화물코드, 화물종류, 총중량, 컨테이너 번호, 봉인 번호, 송장총액, 화물의 고유식별번호 등이다. 화주는 세관에 화물에 대한 수출신고서를 제출한 상황을 문서로(가능하면 전자문서)로 운송인에게 통보해야 한다. 만일 수출신고서 제출시 자료가 미비한 경우 차후에 보충자료를 제공해야 한다.

나) 적하목록신고(Cargo Declaration)

운송인 혹은 운송인의 에이전트는 수출입 장소에서 세관에 적하목록신고를 하여야 한다. 해상 컨테이너 운송의 경우 화물/컨테이너가 선박에 선적되기 전에 적하목록신고를 해야 한다. 다른 운송 수단의 경우에는 운송수단의 도착 이전에 세관 사무소에 신고해야 한다. 보안을 위한 적하목록신고에 필요한 기본적 정보는 선적장소, 캐리어 번호, 컨테이너의 크기, 형태, 그리고 식별번호, 봉인번호, 운송수단국적, 경유국가, 운송수단 식별번호(conveyance reference

number), 운송수수료 정산방법, 최초도착지, 경유국가, 최초도착지 도착시간, 화물형태, 화물의 고유 식별번호 등이다.

다) 수입물품신고(Import Goods Declaration)

수입인 혹은 수입인의 에이전트는 운송수단이 수입지 최초 도착지 세관사무소에 도착하기 전에 수입지 세관에 전자적으로 물품수입신고를 해야 한다. 보안을 위한 수입물품 신고에 필요한 기본적 정보는 수출물품을 신고할 때 제출하는 자료와 동일하다.

라) 위험도가 높은 위탁화물에 대한 정보 교환

일괄적인 통관절차를 위해 공급망상의 모든 세관은 위험도가 높은 위탁 화물에 대해서 효율적인 위험평가 및 화물의 원활한 양도를 위해 세관-세관 데이터 교환을 고려해야 한다. 이러한 전자 교환 시스템은 세관검사 결과를 포함해 수출거래 및 도착 정보를 교환할 수 있어야 한다.

내국법에는 세관이 취합한 정보를 거래국 세관에게 제공할 수 있는 법적 조항을 포함해야 한다. 만일 포함하지 않은 경우에는 이에 대한 조항을 마련해야 한다. 이를 위해서 “The Guidelines for the Development of National Laws for the Collection and Transmission of Customs Information”을 기초로 활용할 수 있다. 또한 기존의 WCO 협약인 “Johannesburg Convention”과 “Model Bilateral Agreement”에 의거하여 위험도가 높은 화물에 대한 정보를 교환할 수 있다.

마) 선적불가(No load), 양륙불가(No unload)

세관은 선적불가 혹은 양륙불가 판정을 받은 위탁화물의 상태를 확인할 수 있는 시스템을 구축해야 한다. 이러한 확인은 위험 평가를 위한 데이터 제출 이후에 규정된 시간 이내에 이루어져야 한다.

바) 시간 제약(Time Limit)

서로 다른 운송모드의 차이점에 의거하여 지역적인 상황이나 기업 프로세스

분석을 통해 국제법에 따라 수출입 지역에서 세관에 적하목록신고 및 물품신고의 제출 시간이 명시되어야 한다. 세관은 운송모드에 상관없이 공인 경제운영자에게 동일한 자격을 부여해야 한다. 그러나 세관은 일반적인 상황이나 특수 상황을 불문하고 다음에 제시한 시간 이전에 신고를 요구해서는 안 된다.

운송 수단	주요 내용
해운	- 컨테이너 화물: 출발지 항만에서의 선적 24시간 전 - 벌크/브레이크 벌크 : 목적지 국가에서의 첫 번째 항만에 도착하기 24시간 전
항공	- 단거리 수송 : 항공기가 이륙할 때 - 장거리 수송 : 목적지 국가 첫 번째 공항에 도착하기 4시간 전
철도	- 목적지 국가 첫 번째 역에 도착하기 2시간 전
도로	- 목적지 국가의 첫 번째 정류장에 도착하기 1시간 전

자료 : 한국해양수산개발원

사) 세계관세기구의 데이터 모델(WCO Data Model)

세관은 운영하고 있는 IT 시스템의 상호 호환성을 유지함으로써 수출입에 필요한 데이터 집합을 정의하는 CDM(Customs Data Model)를 사용할 수 있어야 한다. 또한 CDM은 적하목록신고 및 물품신고를 위해 전자적 서식을 작성되어야 한다.

아) 단일창구(Single Window)

정부는 국제무역에 관련된 데이터를 단일 창구 개념에서 막힘없이 전송하고 국내 및 국제 수준에서 위험에 대한 정보를 교환하기 위해 세관과 거래국의 정부기관들 사이의 협력을 위한 협정서를 마련할 필요가 있다. 이는 전자적으로 필요한 정보를 단일기관, 되도록이면 세관을 통해서 필요한 정보를 주고받는 것을 의미한다. 단일창구 개념은 글로벌 공급체인에서 송장이나 주문서와 같은 문서를 활용하여 무역에 관련된 프로세스와 정보의 흐름을 통합하여 관리하는 장점을 제공한다.

라. 공인 공급망(Authorized Supply Chain)

가) 공인 경제운영자(Authorized Economic Operators)

공인 경제운영자는 최소한의 정보를 세관에 제공할 경우 간소화되고 빠른 통관절차의 권한을 부여받는 업체이다. 이러한 자격을 부여받기 위해서는 세관이 제시한 일정기준을 통과해야 하는데 세관의 요구사항을 만족시킨 충분한 실적을 보유해야 하고, 세관-기업 파트너십 프로그램에 참여하여 공급체인상의 안전한 거래자로 인정을 받아야 한다. 또한 기업 관리를 위한 만족할 만한 시스템을 보유해야 한다. 각국의 세관들은 공인 경제운영자의 권한을 서로 인정해야 한다.

나) 공인 공급망(Authorized Supply Chain)

공인 공급망의 개념은 국제무역에서 공급망상의 모든 협력업체들이 물품의 안전 및 보안 확보와 이에 관련된 정보 관리에서 일정 기준을 준수한 경우에 세관이 이를 인정한 공급망이다. 즉, 출발지에서 목적지까지 공인 공급망을 이동하는 위탁화물에 대해서 수출입시 최소한의 정보로 구성된 일괄신고를 통해 세관절차의 간소화 권한을 부여받는다.

② Standard 2 : 화물 검사 권한

세관은 세관의 영역 내로의 반입, 반출, 혹은 환적 하는 화물을 검사하는 권한을 가져야 한다.

③ Standard 3 : 검사장비의 현대화

화물의 검사를 수행하거나 위험평가를 위해 비파괴 검사 장비(non-instructive inspection equipment)나 방사선 검사 장비를 활용해야 한다. 이러한 장비들은 물류의 흐름에 지장을 주지 않으면서 신속하게 위험도가 높은 화물을 검사할 수 있게 한다. WCO는 첨단기술에 대한 최신 정보를 협력국가에게 지원하고자 자료 은행(data bank)을 운용하고, 첨단장비의 구입 및 운영에 대한 지침서

를 마련하고 있다.

④ Standard 4 : 위험관리 시스템

세관은 잠재적으로 위험성이 내포된 컨테이너를 적발하고 시스템의 자동화를 위해 위험관리 시스템을 반드시 구축해야 한다.

가. 자동 선정 시스템

세관은 국제적으로 위험관리에 사용하고 있는 성공 사례를 바탕으로 자동 시스템을 개발해야 한다. 해상 컨테이너 운송시 이 시스템은 선박에 화물을 선적하기 전에 적용되어야 한다.

나. 위험 관리

위험 관리는 세관에게 위험에 대한 정보를 제공하기 위한 체계적인 관리 절차를 의미한다.

다. WCO 국제 정보 및 정보 수집 전략

효과적인 위험관리 제도는 세관의 통제와 운영에 있어서 정보수집, 처리, 그리고 배포하는 역할을 포함하는 중요한 요소이다.

라. 위험 관리 참고 문서

WCO는 회원국들이 화물 운송에 따른 위험관리를 위해 기존에 기구에서 제정한 협정을 참고할 수 있도록 배려하고 있다.³⁸⁾

⑤ Standard 5 : 위험도가 높은 화물이나 컨테이너

위험도가 높은 화물이나 컨테이너란 보안관련 데이터로부터 위험도가 높다

38) 이 같은 협정은 WCO Risk-Management Guide, WCO Global Information and Intelligence Strategy, WCO Standardized Risk Assessment, General High-Risk Indicators 등임.

고 판단되어지는 것을 의미한다. 세관은 잠재적으로 위험도가 높은 화물을 선별하기 위해 세부적인 절차를 개발해야 한다.

⑥ Standard 6 : 최신 전자 정보

세관은 위험에 대한 정보를 적시에 활용할 수 있도록 화물 및 컨테이너 운송에 사전전자 정보를 필요로 한다.

가. 전산화의 필요성

세관에 보내는 사전정보의 전송은 전산화 된 세관시스템을 필요로 한다. 이 시스템의 사용은 수출입 장소에서의 발생하는 정보의 전자 교환에서도 사용된다.

나. 교토 협약 정보통신기술 지침³⁹⁾

개정교토협약의 일반 부속서에서 표준안 7.1, 6.9, 3.21, 그리고 3.18 등은 세관으로 하여금 전자상거래 기술을 포함하여 정보통신기술을 세관운용에 적용하도록 되어 있다. 따라서 WCO는 세관의 자동화에 관한 자세한 지침을 마련하고 있다. 이러한 교토협약의 정보통신기술 지침은 세관이 새롭게 정보통신 기술 시스템을 개발하거나 기존의 시스템을 향상하고자 할 때 참조한다. 또한 세관의 전산화에 대해서는 WCO에서 정한 기준을 참고한다.

다. 경제운영자 시스템의 사용

정보통신기술 지침은 경제운영자가 새롭게 시스템을 구축하기 보다는 현재 기업이 사용하고 있는 시스템의 사용을 권장한다. 다만 현재의 시스템이 세관의 요구사항을 충족하는지를 검사받아야 한다. 특히 공인 공급망에서 어떤 기밀성 혹은 법적인 문제가 없다면 세관이 온라인으로 기업의 시스템에 접속하여 효과적으로 신뢰성 있는 정보를 교환하여 신속하게 세관절차를 수행할 수 있다.

39) ICT: Information and Communication Technologies의 약자임.

라. 전자 데이터 교환 표준안

교토협약의 정보통신기술 지침은 세관에게 정보의 전자교환 방법을 하나 이상 제공하도록 권장하고 있다. 국제표준 UN/EDIFACT에 의한 EDI 활용이 가장 선호시되는 방법이지만, 세관은 XML과 같은 방법도 고려를 해야 한다. 또한 위험의 정도에 따라 상황은 다르지만 이메일이나 팩스와 같은 방법도 인정하고 있다.

마. WCO 데이터 모델

WCO 관세 데이터 모델의 데이터 구성에 따라 세관에 적하목록신고서와 물품신고서를 제출해야 하는 경제 운용자는 WCO 관세 데이터 모델의 전자 메시지 규격을 준수해야 한다.

바. 정보통신 기술 보안

공용 네트워크를 통해 정보를 전자적으로 전송함에 있어서 정보통신기술의 사용은 특히 세밀한 정보통신기술 보안전략을 필요로 한다. 따라서 이러한 정보통신기술 보안 사항은 세관의 전체적 공급망 보안 전략의 한 부분으로 인식되어야 한다. 효과적이고 효율적인 정보기술 전략을 수립하기 위해서 세관은 위험평가를 받아야 한다. 교토 정보통신기술 지침은 정보 및 정보시스템의 가용성, 무결성, 그리고 기밀성에 대한 전반적인 내용들을 포괄하고 있다.

사. 디지털 서명

공급망의 보안을 확보하는 정보통신 기술 보안의 핵심요소 중 하나는 디지털 서명이다. 디지털 서명 혹은 공개 키 기반(Public Key Infrastructure)은 송수신되는 정보의 보안을 유지하기 위해 중요한 역할을 할 수 있다. 이러한 보안이 확보되면 통합세관관리의 일련 프로세스에서 무역업자들은 사전에 수출국의 세관뿐만 아니라 수입국의 세관에 각종 신고서를 제출할 수 있는 가능성을 제공한다. 경제적 운용자에게 디지털 인증을 세관들 상호 간에 인정을 한다

면, 보안에 대한 검증이 더욱 요구되지만 무역업자에게는 무역거래에 있어서 효율성을 더욱 보장할 수 있다. 이러한 이유 때문에 세관은 전자적 정보 송수신, 세관의 검증, 그리고 관계된 규정 정보에 관계된 WCO 권장사항을 따르도록 하고 있다.

아. 능력향상

세관 당국은 WCO에서 제정한 프레임워크의 기준을 이행하는 데 필요한 조직 등 능력을 갖추고 있어야 한다.

자. 데이터 프라이버시 및 보호

세관 대 세관 혹은 세관과 민간 기관과의 데이터 교환은 데이터 프라이버시 및 보호에 관계된 정부 기관과의 사전 협의를 한 후에 이루어져야 한다. 프라이버시에 대한 개인의 권리 보호와 무역거래의 기밀성을 보장하기 위해 데이터의 프라이버시 및 보호 법률이 제정되어야 한다. 따라서 이 법률은 세관이 데이터를 수집하거나 전송할 때 기밀성과 보안에 관한 조항을 포함해야 한다. 또한 이 법률은 정보에 관계된 자연인 혹은 법인에게 특정한 권리를 보장해야 한다.

데이터 보호와 기밀성은 현재 WCO에서 따르고 있는 요하네스버그 협약(Johannesburg Convention)과 모델양자간협정(Model Bilateral Agreement) 등에 언급되어 있다.

⑦ Standard 7 : 타킷팅과 의사교통

가. WCO 글로벌 정보와 지식 전략

WCO 글로벌 정보와 안보전략(WCO Global Information and Intelligence Strategy)의 제4장에는 표준위험평가(Standardized Risk Assessments : SARs)에 필요한 조항이 포함되어 있다. 표준위험평가는 지식전략에서 중요한 부분이

며, 세관에게 물품이나 운송수단의 위험 잠재성을 사전에 파악하고 검사하는데 필요한 위험지수를 제공한다.

나. WCO 표준위험평가서

표준위험평가서는 5개의 영역으로 나누어 위험지수를 평가하도록 되어 있다. 운송모드, 이익 보호, 의약품 등, 보안, 그리고 기타 금지 및 제한 등이 그것이다. 각 영역별로 표준목표 평가기준이 설정되어 있다. 또한 각 영역은 정기적으로 최신의 정보로 갱신되어지는 다수의 하부 위험지수로 나누어져 있다.

다. WCO 일반위험평가서

WCO 일반위험평가서는 일반적인 방법으로 세관이 관세위반을 검사하기 위한 주요검사 항목에 대한 지수를 포함하고 있다. 서류의 제목들은 운송인 목록 세부 사항, 위험도가 높은 국가 판단 기준, 높은 위험 조건을 명시한 상품과 운송 요인, 은폐목적으로 사용된 알려진 위험도가 높은 물품, 테러에 이용될 잠재성이 높은 위험물품 명세서 등이다.

라. 세관을 위한 위험지수에 관한 WCO 안내서

해적과 위조물에 대한 높은 위험을 지적하는 주요 요소들의 목록이 안내서에 포함되어 있다.

마. 법적 근거

공동 목표설정과 심사는 선적 보안과 국경에서의 조직화된 범죄에 효과적으로 대처하기 위해 세관에 의해 행해지는 활동을 말한다. 이러한 공동 활동을 위한 규칙과 조건은 세관 사이에 통상적으로 확립되어야 한다. 요하네스버그 협약과 모델 상호협정과 같은 WCO 도구들은 국제 혹은 양자간 협력을 지원하는 조항들을 포함하고 있다.

⑧ Standard 8 : 성과 측정

세관은 화물에 대한 보안검사 결과에 대한 통계적 분석 자료를 관리해야 한다. 이 자료들은 선적에 대한 검사 횟수, 고위험 화물에 대한 검사 횟수, 비파괴 검사장비에 의한 고위험 화물 검사 횟수, 비파괴 검사장비 및 물리적 수단에 의한 고위험 선적의 검사 결과, 물리적 검사 수단에 의한 고위험 화물의 검사 결과, 그리고 통관시간과 이에 대한 긍정적 및 부정적 결과 등이다. 또한 이러한 자료들은 세계관세기구가 종합 · 관리한다.

⑨ Standard 9 : 보안 평가

세관은 국제 공급망에서의 물품이동에 관계된 보안평가를 실시하고, 평가 결과에 결함이 확인되면 관련이 있는 다른 기관들과 협조하여 신속하게 해결한다.

⑩ Standard 10 : 종업원의 무결점

세관과 관계기관들은 종업원의 무결점을 위한 실책을 방지하고 무결점의 결함을 확인하고 제거하는 프로그램의 필요성을 인식해야 한다.

가. WCO 부패방지 협정 활용

WCO는 세관들을 위해 부패방지시스템을 구축하기 위해 기존에 협약을 제정하여 시행하고 있는데,⁴⁰⁾ 이 같은 협정을 프레임워크를 시행하는데 참고할 수 있다.

나. 훈련

공급망에서의 보안 확보 및 국제교역의 촉진은 세관이나 공급망에서의 관련 기관에서 고도의 훈련된 인력을 필요로 한다. 따라서 세관은 효율적인 세관 통제와 전자 정보에 관련된 훈련을 전 종업원을 대상으로 정기적으로 실시하여야 한다.

40) 이 분야의 WCO 대표적인 규정은 개정된 아루사 선언(Revised Arusha Declaration)임.

⑪ Standard 11 : 수출 보안검사

세관은 수출화물에 대해 수입국이 합리적인 절차에 따라 위험도가 높은 컨테이너의 보안 검사를 요구할 경우 이에 따라야 한다.

가. 검사요구

수입국 세관이 위험평가에 의거하여 위험도가 높은 컨테이너나 화물로 인지한 경우에 수출국의 세관에 선적 전에 검사를 요구할 수 있다.

나. 법적근거

수입국 세관은 WCO가 제정한 요하네스 협약이나 양자 모델 협약에 따라 수출국 세관 당국에게 수출 컨테이너 화물에 대한 검사를 요청할 수 있다.

(3) 세관-기업 Pillar

각국의 세관은 공급망을 활용한 국제무역에서의 안전과 보안을 확보하기 위해서 민간기관들과 파트너십을 구축해야 한다. 이 세관-기업 Pillar는 공급망에서 높은 보안 수준을 제공하고 있는 기업을 대상으로 국제 물류보안 시스템을 구축하는 것이다. 이러한 높은 수준의 보안을 제공하는 기업에게는 빠른 화물 처리와 같은 혜택을 부여 받는다. 이 프레임워크는 공급망에서 보안 파트너로서의 공인 자격을 획득하는 기준들을 명시하고 있다. 이 기준들은 위험평가, 보안위험에 대한 보안계획, 통신계획, 설비보안, 컨테이너 보안, 운송수단, 정보시스템 보안 등이다.

(4) Pillar 2 Standards

① 파트너십

국제무역 공급망에서 활동하는 공인경제운용자는 사전에 제시된 보안표준과 모범 사례에 따라 자체적인 보안평가를 수행할 수 있다. 세관-기업의 파트너십

프로그램은 공인 경제운영자가 운용하고 있는 비즈니스 모델을 바탕으로 보안 계획에 대한 유연성과 맞춤형을 부여해야 한다. 세관과 공인 경제운영자는 동시에 적절한 파트너십 보안측정치를 결정하고 문서화해야 한다. 이러한 파트너십 보안측정치는 경제운영자에 의해서 실행되고 관리되어야 한다. 공동합의에 의해 작성된 관세-기업의 파트너십 문서는 문서화되어야 한다. 또한 공인 경제운영자의 비즈니스 모델, 즉 공인 경제운영자의 비즈니스 파트너, 생산자, 공급자, 그리고 판매자가 WCO 표준안에 제시된 공인 경제운영자의 프로세스와 보안측정치에 대한 정기적인 재검사가 시행되어야 한다. 재검사는 비즈니스 보안에 관계된 협정에 제시된 보안 절차를 따라야 한다.

② Standard 2 : 보안

공인 경제운영자는 현재 운영하고 있는 보안 시스템에 외부 성공 사례가 있을 때는 이를 적용한다. 공인 경제운영자는 건물의 자체 보안뿐만 아니라 건물 외곽 및 내부의 보안을 감시, 통제하고 각종 시설에 공인되지 않은 사람의 출입을 제한해야 한다. 건물 출입시 보안을 증명할 수 있는 증명서나 출입증 제도를 운용하여야 한다. 정보 시스템에 대한 데이터 사용에도 비밀번호를 부여하는 등 보안을 확보해야 한다. 그리고 정기적인 정보시스템 보안 훈련을 실시해야 한다. 개인보안 프로그램은 종업원에 대한 신원조사도 포함되어야 한다.

③ Standard 3 : 인증(Authorization)

세관은 무역관계자 대표들과 함께 공인 경제운영자와 같은 인증 기업에게 부여하는 혜택에 관한 품질인증 및 적합성을 부여하는 프로세스를 구축할 의무가 있다. 이 프로세스는 공인 경제운영자가 보안 시스템을 구축하기 위해 투자한 자본에 대해서 혜택을 받는다는 점을 인식하는 점을 고려해야 한다. 예로서, 공인 경제운영자가 누릴 수 있는 혜택은 신속한 통관이나, 검사 또는 위험 대상에 대한 평가가 용이하다는 점을 들 수 있다.

④ Standard 4 : 장비

공급망에 참여하는 모든 기관은 첨단장비를 사용하여 화물 및 컨테이너의 무결성을 위해 노력해야 하는 의무가 있다. 공인 경제운영자는 국제협약, 즉 1972 Customs Container Convention, Customs Convention on International Transport of Goods under Cover of TIR Carnets 등이 제시한 규정에 부합하는지 확인하여야 한다. 세관은 다양한 혜택 부여 방법을 통해 화물 및 컨테이너의 보안을 확보하기 위해 최신의 장비 사용을 적극 장려해야 한다. 또한 공인 경제운영자는 컨테이너 봉인방법에 대한 규정을 문서화하여 운영해야 한다.

⑤ Standard 5 : 통신

세관은 보안표준을 간소화하고 공급망 보안에서 성공 사례를 촉진하고자 정기적으로 세관-기업의 파트너십 프로그램을 최소화할 의무가 있다. 세관은 공인 경제운영자와 협조하여 예기치 않은 사고에 대비하여 공인 경제운영자를 포함한 에이전트의 전화번호를 확보하여 긴급 연락망을 구축할 수 있는 절차를 수립해야 한다. 또한 세관은 국가적 혹은 지역적 수준에서 국제 공급망에 참여하고 있는 주체들과 관세규정, 절차 등에 관한 안전들에 대해 정기적으로 서로 의견을 교환하는 것이 필요하다.

⑥ Standard 6 : 원활화

세관은 국제무역의 원활화 및 세관 업무와 관련된 공급망의 보안을 극대화하기 위해 공인 경제운영자와 협력하여 업무를 처리할 의무가 있다. 세관은 화물의 흐름을 원활히 하고 위험화물을 검색하는 등의 관세 업무를 수행함에 있어서 필요한 정보를 능률적으로 처리하기 위한 조항을 추가하거나 개정해야 한다. 또한 세관은 추가 조항이나 개정사항에 대해 관련 기업들이 이익을 제기할 수 있는 절차를 마련해야 한다.

3) 시사점

WCO의 물류보안 제도는 100여개 국가에서 시행하기로 합의함에 따라 사실상 세계 규범으로 확대되고 있다. WCO 프레임워크의 주요 목적은 물류 전반에 있어 보안 확보 및 원활한 무역 활동을 위해 각국의 세관 및 기업들과의 공조체제를 구축하는 표준을 마련하는 데 있다. 핵심 내용은 전자적 화물 정보의 원활한 공유, 보안위협에 대한 일관된 위험관리체계 마련, 최신 장비를 활용한 비파괴 검사 수행, 보안 기준을 이행할 경우 기업에 부여하는 특혜 등이다.

WCO가 제시하는 내용은 물류 전반을 통합적으로 관리하는 방향으로 전체적으로 구성되어 있다. 따라서 현재 우리나라에서 이루어지고 있는 항만이나 공항 위주의 보안 관리가 내륙으로 확대되어 화물을 선적하는 시점에서부터 관리되는 체계적인 시스템을 구축해야 된다는 점을 인식해야 한다. 또한 WCO의 주요 구상 가운데 한 부분은 공인 경제운영자(Authorized Economic Operator) 자격을 얻는 국제표준 안이다. 물류에 참여한 기관이 이 자격을 취득하면 전 세계에서 통관절차의 간소화 혜택이 보장받을 수 있게 된다. 더불어 WCO는 첨단 보안장비 사용을 권유하고 있어 이에 대처하기 위해 법제도 정비, 보안장비 개발, 정보관리시스템 개발, 전문 인력 양성 등 다방면의 준비가 필요하다.

3. 국제표준화기구(ISO)

1) ISO의 물류보안 인증

국제표준화기구(International Organization for Standardization, ISO)는 각국의 표준제정 단체들의 대표들로 구성된 국제기구이다. 비정부 기구이지만 국제표준화기구가 정한 규격은 보통 국제협약이나 국가 표준제정을 통해 제도화되기 때문에 다른 비정부 기구보다 영향을 크게 행사하고 있다. 참가자는 회원국

에서의 표준제정 단체와 주요 기업 등이다. ISO는 현재 물류보안과 관련하여 크게 두 가지 규정을 제정하고 있다. 컨테이너 보안 표준을 제정하는 것과 기업의 보안관리 표준을 작성하는 것이 그것이다. 전자의 경우 아직 내용이 확정되지 않았으므로 이 곳에서는 후자를 중심으로 논의를 전개한다.

국제표준화기구는 기업의 보안관리표준의 필요성에 부응하여 ISO/PAS 28000 협약을 발표하였다. ISO/PAS란 ISO Publicly Available Specification을 줄인 약어이다. 여기서 PAS란 ISO의 전문가들이 모인 위원회에서 잠정적으로 합의한 협약으로서 회원국의 50% 이상이 동의하면 발표가 된다. 그 후 3년 후에 재검토 과정을 거친 후 국제 표준안으로 확정할 것이지를 결정한다. 따라서 공급망의 보안관리⁴¹⁾ 시스템을 위한 표준안인 ISO/PAS 28000은 PAS에 속한 협약으로 2005년 11월 15일에 발표되었다. 이 협약에 적용된 방법론은 계획-실행-검토-조치(Plan-Do-Check-Act, PDCA)의 절차에 기초하고 있다.

ISO/PAS 28000은 크고 작은 모든 조직이 운영하고 있는 공급망의 전 프로세스, 즉 제조, 서비스, 보관·운송 전 분야에 적용이 가능하다. ISO/PAS 28000은 기본적으로 다음 사항들을 달성하는 것을 목적으로 하고 있다.

- i) 보안관리 시스템의 구축, 실행, 유지, 그리고 개선
- ii) 보안관리정책과의 적합성 확립
- iii) 타 기관에게 적합성을 증명
- iv) 공인 삼자인증기관에 의한 보안관리 시스템의 인증
- v) ISO/PAS 28000에 의한 자가 진단 가능 등이다.

ISO/PAS 28000에 규정되어 있는 보안관리 시스템이 구축되는 경우 인증기관에서 인증을 받게 되면 해당기업은 일정한 보안자격을 갖춘 것으로 인정된다. 일반적으로 인증은 국제선급연합회(IACS)에 소속되어 있는 각국의 선급에서 시행하는 것이 원칙이다. 2006년 11월 현재 ISO/PAS 28000에 따라 인증을 받은 곳은 아랍에미리트에 있는 두바이의 제벌 알리 항만이다. 우리나라의

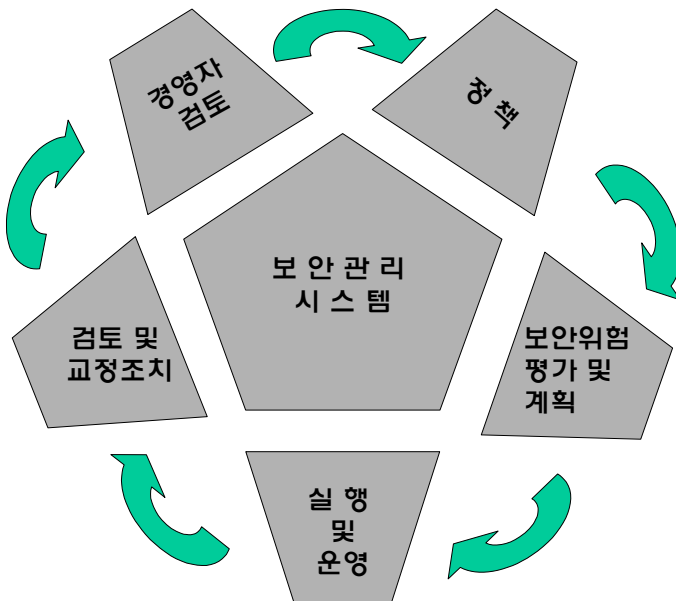
41) 시스템적이고 일원화된 활동을 통해서 조직이 조직의 위험과 잠재적인 위험에 최적으로 대처하는 것을 말한다.

부산 신항만(PNC)도 최근 ISO/PAS 28000에 따라 보안인증을 받는 방안을 한국선급(KR)과 협의하고 있는 것으로 알려졌다. ISO/PAS 28000에 규정되어 있는 기업의 보안 관리시스템을 검토하면 다음과 같다.

2) ISO의 보안관리 시스템

ISO의 보안관리 시스템은 정책(policy),⁴²⁾ 보안위협평가와 계획(security risk assessment & planning), 실행 및 운영(implementation & operation), 검사 및 수정(checking & corrective action), 경영자 검토(management review) 등으로 구성되어 있다(<그림 3-1> 참조).

〈그림 3-1〉 보안관리 시스템의 구성요소



42) 조직의 정책, 법적 제약과의 일관성을 유지하면서 보안관리에 대한 조직이 추구하는 방향을 의미함.

(1) 일반 사항

조직은 보안위험을 식별하고 그 영향을 통제하는 한편, 보안 위험을 최소화하고자 효과적인 보안관리 시스템을 구축, 실행, 유지, 그리고 지속적으로 개선해야 한다. 이를 위해 먼저 보안관리 시스템의 범위를 명확히 정의해야 한다. 또한 조직이 보안관리 절차를 일부를 외부에 위탁할 경우 이를 통제할 수 있어야 한다.

(2) 보안관리 정책

조직의 최고 경영진은 전 조직의 보안관리 정책을 수립하고 권한을 부여해야 한다. 이 정책이 가져야 할 특징은 다음과 같다.

- 가) 조직의 다른 정책들과 상충되는 점이 없어야 한다.
- 나) 조직은 보안관리 정책에 따라 보안관리의 목적, 달성목표, 그리고 프로그램을 포함하는 전체 프레임워크를 구축해야 한다.
- 다) 보안관리 정책은 전조직의 보안위협 및 위협관리 프레임워크와 상충되는 점이 없어야 한다.
- 라) 정책은 조직에 미칠 위험에 상응하는 규모가 설정되어야 한다.
- 마) 보안관리 목적이 명확히 정의되어야 한다.
- 바) 보안관리 절차의 지속적인 개선을 보장해야 한다.
- 사) 정책은 최고 경영진으로부터 승인을 받아야 한다.
- 아) 정책은 문서화되어 실행, 관리되어야 한다.
- 자) 정책은 종업원뿐만 아니라 계약업자, 방문자를 포함한 제삼자도 보안관리 의무가 숙지하도록 의사소통되어야 한다.
- 차) 정책은 조직에 영향을 미치는 이해관계자들에게 공개되어야 한다.
- 카) 보안관리 시스템에 영향을 주는 요인, 즉 인수 혹은 합병, 조직 내 변화가 있을 때 재검토해야 한다.

(3) 보안위협 평가 및 계획

① 보안 위협 평가

조직은 보안위협뿐만 아니라 보안관리에 관련된 위협과 위험을 식별, 평가하고 필수 경영관리 측정치의 확립 및 이행하는 지속적인 프로세스를 개발하고 유지해야 한다. 보안위협 및 위험인식, 평가와 관리방법들은 최소한 현실에 운영 가능하여야 한다. 중요 평가 항목들은 다음과 같다.

- 가) 물리적 고장으로 인한 위협과 위험(기술적 고장, 우발적 손상, 의도적 손상 혹은 테러/범죄 행위와 같은 내용을 포함)
- 나) 조직의 운영에 영향을 미치는 위협과 위험(조직 운영에 있어서의 성능, 조건, 혹은 안전에 영향을 미치는 활동, 보안통제, 휴먼 에러 등을 포함)
- 다) 폭풍, 홍수 등의 자연 환경적 사건(보안측정과 장비사용에 비효율적으로 영향을 미치는 요소를 포함)
- 라) 조직의 외적인 요인, 즉 공급자로부터 공급받은 장비 혹은 서비스를 포함
- 마) 법적 요구사항 불이행 및 조직의 명성을 손상 시킬 수 있는 위협이나 위험
- 바) 교체 및 유지보수를 포함한 보안장비의 디자인과 설치
- 사) 정보와 데이터의 관리 및 커뮤니케이션
- 아) 운영의 연속성에 대한 위협

조직은 이들 평가항목에 대한 평가치와 통제효과에 대한 결과를 이용하여 다음과 같은 항목의 입력 자료로 활용해야 한다.

- 가) 보안관리 목적과 대상
- 나) 보안관리 프로그램
- 다) 보안 장비 디자인, 규격, 그리고 설치를 위한 요구사항 결정
- 라) 인력의 교육수준 등을 포함한 자원의 적절한 배분
- 마) 인력훈련 필요성 및 보유기술 설정
- 바) 운영적 통제의 개발

사) 전 조직의 위협과 위험을 관리하기 위한 프레임워크

조직은 위에서 언급한 정보를 문서화하고 주기적으로 최신의 자료로 갱신해야 한다. 위협과 위험을 감지하고 평가하기 위해 조직이 활용하는 방법론은 i) 수동적이기보다 예방차원에서 범위, 내용, 시기 등을 고려하여 정의되어야 한다. ii) 보안 위협과 위험에 관련된 정보를 수집해야 한다. iii) 위협과 위험을 등급화하여 회피하거나 제거할 수 있는 정보를 제공해야 한다. iv) 이행함에 있어서 효과성과 적기성을 확보하는 행동에 대한 모니터링을 할 수 있어야 한다.

② 법률 및 보안규정

조직은 연계된 보안관리 법률 및 보안규정에 대한 최신의 정보를 확보하여 이 정보가 조직의 보안위협과 위험에 어떻게 영향을 미치는지 검토할 수 있는 절차를 마련해야 한다. 또한 이러한 정보는 종업원뿐만 아니라 관련된 제삼자들도 공유할 수 있어야 한다.

③ 보안관리 목적

조직은 내부적으로 문서화된 보안관리 목적을 수립하고 실행하여 지속적으로 관리해야 한다. 보안관리 목적은 조직의 정책으로부터 정의되어야 할 뿐만 아니라 정책과 일관성을 가져야 한다. 목적을 정의하고 검토하기 위해서 조직은 다음과 같은 사항을 고려해야 한다. i) 법, 법률, 그리고 보안규정, ii) 보안 관련 위협과 위험 요소, iii) 기술적인 요소, iv) 재정, 운영, 비즈니스 요구 사항 및 v) 주주의 의견 등이다.

그리고 보안관리 목적은 i) 지속적인 발전을 위해 조직의 공약과 일치해야 한다. ii) 가능하면 계량화하여야 한다. iii) 종업원을 포함해서 계약업자와 같은 관련된 제삼자들과 의사교환되어야 한다. iv) 보안관리 정책과의 모순점이 발생하지 않도록 정기적으로 검토되어야 하며, 필요한 경우 개정해야 한다.

④ 보안관리 대상

조직은 필요성에 따라 문서화된 보안관리 대상을 수립, 실행하여 지속적으로 관리해야 한다. 이 목적은 보안관리 목적으로부터 정의되어야 할 뿐만 아니라 목적과 일관성을 가져야 한다. 이러한 목적은 i) 적절하게 구체화되어야 한다. ii) 가능하면 구체적이고, 측정 가능하고, 달성 가능하여, 계획적으로 관리되어야 한다. iii) 종업원을 포함해서 계약업자와 같은 관련된 제삼자들과 의사교통 되어야 한다. iv) 보안관리 목적과 모순점이 발생하지 않도록 정기적으로 검토되어야 하며, 필요하면 개정되어야 한다.

⑤ 보안관리 프로그램

조직은 보안관리 목적과 대상의 목표를 달성하고자 보안관리 프로그램을 수립하고 실행하여 지속적으로 관리해야 한다. 이 프로그램을 최적화하고 우선순위를 정해야 한다. 그리고 조직은 이러한 프로그램에 대한 효율적이고 비용 효과적인 실행방법을 제공해야 한다. 이 같은 프로그램을 문서화 하는 한편, 문서화할 때는 다음 사항을 고려한다. i) 보안관리 목적과 대상의 목표를 달성하고자 책임과 권한을 명시해야 한다. ii) 보안관리 목적과 대상의 목표가 달성되기 위해 수단과 시간적인 계획을 포함한다.

(4) 수행과 운영

① 보안관리를 위한 조직구조, 권한, 책임

조직은 보안관리 정책, 목적, 대상, 그리고 프로그램의 목표와 일관성 있게 조직의 역할 분담, 책임, 권한을 수립하고 관리해야 한다. 이러한 역할분담, 책임, 권한에 대한 개념을 정립하고 문서화한다. 그리고 실행과 유지보수를 책임지고 있는 담당자와 의사교통되어야 한다. 최고 관리자들은 보안관리 시스템을 개발 및 실행하고 지속적인 발전을 위해 확고한 의지를 표방하는 증거를 마련해야 한다. 이러한 증거를 마련하기 위한 방법은 다음과 같다.

- i) 보안관리만을 담당하는 최고 관리자를 임명하고, 이 관리자는 조직의 보안 관리 시스템의 계획수립, 유지보수, 문서화 등에 관한 전반적 사항에 책임을 진다.
- ii) 보안관리 목적과 목표치를 달성하고자 권한을 가지는 관리자를 임명한다.
- iii) 조직의 이해관계자들의 요구 및 기대사항들을 파악하고, 필요한 경우 적절한 조치를 취한다.
- iv) 조직 자원의 가용성을 확인한다.
- v) 보안관리 정책, 목적, 목표치, 프로그램이 조직의 다른 영역에서 영향을 끼치는 역효과를 고려한다.
- vi) 조직의 다른 부서에서 생성된 보안 프로그램이 보안관리 시스템을 보완하는 효과를 고려한다.
- vii) 조직의 정책에 순응하기 위해 보안관리 요구사항을 충족하는 기준 및 조직을 설정한다.
- viii) 조직에 위협 및 위험 평가에 보안에 관련된 위협 및 위험을 평가하고 포함하는 것을 보장한다.
- ix) 보안관리 목적, 목표치, 프로그램의 실현가능성을 보장해야 한다.

② 자격, 교육훈련, 인식도

조직은 보안장비 및 보안절차에 관한 계획수립, 운영, 관리를 담당하고 있는 개인이 충분한 교육수준, 훈련, 그리고 경험을 보유하고 있는지를 확인해야 한다. 그리고 조직은 보안 관계자를 위한 프로그램을 마련하고 운영해야 한다. 이 프로그램에서 고려해야 할 사항은 다음과 같다. i) 보안관리 정책 및 프로세스, 그리고 보안관리 시스템의 요구사항을 준수해야 하는 중요성을 인식, ii) 보안관리 정책 및 프로세스 그리고 보안관리 시스템의 요구사항을 순응하기 위한 개인들의 역할과 책임, iii) 조직의 운영 절차 이외에 조직의 보안에 관한 잠재적 중요성 인식, 그리고 자격 및 교육훈련에 관한 기록 관리 등이 이에 해당된다.

③ 의사소통

보안관리 정보는 조직의 일원을 비롯하여 제삼자, 그리고 이해 관계자들과 공유되도록 해야 한다. 보안과 관련된 정보가 무단으로 외부에 유출되는 것을 방지하기 위하여 배포하지 전에 충분한 검토를 거쳐야 한다.

④ 문서화

조직은 보안관리 문서화 시스템을 개발하여 운영해야 한다. 이 시스템에 포함되어야 할 사항은 i) 보안 정책, 목적, 그리고 목표치, ii) 보안관리 시스템의 범위, iii) 보안관리 시스템의 구성요소, 구성요소 간의 관계, 그리고 참고사항, iv) 국제 표준을 비롯한 각종 보안 관련 자료, v) 조직이 마련한 보안위협 및 위협에 관련된 효과적인 계획, 운영, 통제 절차 등이다. 이와 함께 조직은 정보에 관한 보안의 수준을 정하고, 권한을 가진 자만 이용할 수 있게 한다.

⑤ 문서와 데이터 통제

조직은 ISO의 보안관리 시스템에 필요한 모든 문서, 데이터, 정보를 통제하기 위한 절차를 마련하고 관리해야 한다. 이를 위해 고려할 사항은 다음과 같다.

- i) 문서, 데이터, 정보는 사용 권한을 가진 자가 관리하고 이용해야 한다.
- ii) 문서, 데이터, 정보는 주기적으로 검토되고 필요시 변경한다.
- iii) 문서, 데이터, 정보의 최신 버전은 보안관리 시스템이 운영되는 모든 수준에서 사용 가능해야 한다.
- iv) 사용이 불가능한 문서, 데이터, 정보는 신속하게 폐기해야 한다.
- v) 법적인 혹은 지식보전을 위해 보관된 문서, 데이터, 정보는 분리해서 관리한다.
- vi) 문서, 데이터, 정보는 안전하게 관리하고, 가능하면 전자적 형태로 백업하여 복사한다.

⑥ 운영 통제

조직은 다음과 같은 사항의 목적을 달성하기 위해 관련된 운영과 활동을 확립해야 한다. 프레임 워크에서 구체적으로 정한 목적은 i) 조직의 보안관리 정책, ii) 규정된 보안위협과 위협의 통제, iii) 법률 및 그 외 보안규정 요구사항을 준수, iv) 조직의 보안 관리 목적, v) 조직의 보안관리 프로그램을 실행, vi) 공급망 보안의 요구 수준 만족 등이다. 또한 이러한 운영과 활동을 수행하기 위해 조직이 필수적으로 수행해야 하는 점은 i) 문서화된 절차의 수립, 이행, 그리고 유지, ii) 수직적으로 상위 공급망에서 발생할 어떠한 위협에 대해서 수준을 평가하여 조직 및 하위 수준의 공급망에 미칠 위협의 경감, iii) 보안에 영향을 미칠 수 있는 제품이나 서비스에 대한 기준 수립 및 유지 등이다.

⑦ 긴급사태 준비, 대처방안, 보안 회복

조직은 보안사고 및 긴급 상황에 대한 준비, 대처방안, 회복방법을 위한 계획을 수립하고 이에 대한 절차를 마련해야 한다. 더불어 긴급 상황 발생을 사전에 방지하고 경감할 수 있는 대책을 마련해야 한다. 이러한 계획이나 절차에 포함되어야 내용은 보안사고 및 긴급 상황 동안이나 사후에 요구되는 장비, 시설, 그리고 서비스에 준비와 관리에 대한 정보 등이다. 그리고 수립된 계획과 절차의 효과를 정기적으로 점검해야 한다.

(5) 검사와 교정조치

① 보안성과와 감시

조직은 보안관리 시스템을 감시하고 측정하는 절차를 수립하고 이를 관리해야 한다. 또한 보안성과능력에 대한 감시와 측정에 관한 절차를 수립하고 이를 관리해야 한다. 그리고 핵심 보안성과 요소에 대한 감시와 측정 횟수를 보안 위협과 위험을 고려하여 설정해야 한다. 이러한 절차는 다음 사항에 대한 내용을 포함해야 한다.

- i) 조직의 필요에 따라 질적 성과자료뿐만 아니라 양적 성과자료를 제공
- ii) 조직의 보안관리 정책, 목적, 그리고 목표치가 제대로 작동하고 있는지 감시
- iii) 보안관리 시스템, 운영통제기준, 관련 법률, 그 외 보안관련 규정의 요구 사항과 조화를 이루는지 감시하는 성과의 사전 측정치를 제공
- iv) 보안관련 오류, 실패, 사고 등을 감시하기 위한 성과의 반응 측정치를 제공
- v) 보정 및 예방 방지 분석 결과의 감시 및 측정 그리고 데이터 기록

② 시스템 평가

조직은 보안관리 계획, 절차, 그리고 능력을 정기적인 검토, 검사, 과거 경험, 성과측정 등을 적용하여 평가해야 한다. 또한 관련 법률, 최신 기업 사례, 조직의 정책과 목적과의 적합성도 주기적으로 평가해야 한다. 그리고 이러한 주기적인 평가 결과를 기록하여 보존해야 한다.

③ 보안관련 실패, 사고, 교정, 예방조치

조직은 다음 사항에 대한 책임과 권한을 설정하기 위한 절차를 수립, 이행하고 이를 관리해야 한다.

- i) 잠재적 보안 실패 상황에 대한 평가 및 예방조치
- ii) 보안관련 조사(잘못된 정보나 실패가 예상되는 경우를 포함한 실패 상황, 규정을 준수하지 않는 경우)
- iii) 보안 실패, 사고 혹은 불이행으로 발생한 영향을 경감하기 위한 조치
- iv) 교정 조치의 개시 및 완료
- v) 교정 조치의 효과성에 대한 확증

제안된 교정 및 예방 조치들은 실행하기 전에 보안위협과 위험평가 절차를 통해서 검토되어야 하는데, 다만 공공안전과 생명이 위급한 상황은 제외한다. 그리고 교정 및 예방 조치들은 보안관리 관련 위협과 위험의 크기에 비례하여

취하여야 한다. 조직은 교정 및 예방조치에 의한 변화들을 문서로 기록하여야 한다.

④ 기록 자료의 관리

조직은 보안관리 시스템, 조직의 표준, 그리고 보안성과 측정치의 적합성을 확인하기 위한 자료를 기록하고 관리해야 한다. 그리고 조직은 기록한 자료의 검정, 저장, 보호, 복구, 보존, 폐기를 위한 절차를 수립, 이행, 관리해야 한다. 이러한 기록들은 명료하고, 증명할 수 있고, 추적 가능하게 유지되어야 한다. 전자 혹은 디지털 문서는 고쳐질 염려 없게 관리되고, 안전하게 보관되어야 한다. 또한 사용 권한을 가진 자만이 접근 가능해야 한다.

⑤ 감사

조직은 보안관리 감사 프로그램을 수립, 이행하고 관리해야 한다. 또한 감사 프로그램은 계획된 주기에 따라 이행되어야 한다. 감사의 목적은 다음과 같다.

- 가) 보안관리 시스템이 i) 보안관리를 위해 계획되고 작동되고 있는지, ii) 올바르게 이행되고 관리되었는지, iii) 조직의 보안관리 정책과 목적에 부합하게 효과적으로 운영되었는지를 감사하는 데 초점을 맞춘다.
- 나) 시행된 감사의 결과와 문제점에 대한 조치를 검토하고, 감사 결과를 경영자에게 제공하고, 보안장비와 인력이 적절히 배치되었는지 확인한다.

(6) 경영진의 검토와 지속적 개선

최고경영진은 조직의 보안관리 시스템의 적절성과 효과성을 지속적으로 확보하기 위해 주기적으로 이를 점검해야 한다. 점검할 사항은 시스템의 개선할 점과 보안관리 시스템에서 고쳐져야 할 부분들을 포함한다. 또한 최고경영진의 검토한 결과를 관리해야 한다. 최고경영자의 검토에 필요한 내용은, i) 감사 결과 및 법적인 정합성의 평가, ii) 불만족 내용 등을 포함한 외부 의견 반영, iii) 조직의 보안성과, iv) 보안관리 목적과 목표치의 만족 정도, v) 교정 및

예방조치 상황,vi) 이전의 검토 결과에 따른 조치 상황, vii) 보안관리에 관계된 법적인 변화 등을 포함한 상황 변화, viii) 개선 방향 등이다.

한편, 최고경영자의 검토한 결과물은 보안관리 정책, 목적, 목표치, 그리고 보안관리 시스템에 대한 변경 사항에 대한 의사결정 내용이나 조치 결과를 포함한다.

3) 시사점

ISO는 각국의 표준제정 단체들로 구성된 비정부 기구이지만 국가 표준제정을 통해 제도화되기 때문에 영향을 크게 행사하고 있다. ISO/PAS 2800의 보안관리 시스템은 물류의 프로세스, 즉 제조, 보관, 운송 등 전 분야에 적용가능하게 디자인 되어 있다. 이 시스템이 구축되면 보안자격을 갖춘 것으로 인정되어 전 세계적으로 보안 적합성을 증명할 수 있게 된다.

따라서 동북아 항만들이 치열한 경쟁을 벌이고 있는 시점에서 ISO에 의한 보안 인증은 항만 경쟁력 제고, 즉 ‘안전 터미널’ 이라는 인식으로 활용될 수 있다. 현재 이 표준에 따라 인정을 받은 곳은 아랍에미리트에 있는 두바이의 제별 알리 항만인 것으로 알려져 있다. 이를 위해 보안인증을 위한 전문 업체 발굴, 보안 전문가 육성 및 교육 등에도 관심이 모아져야 한다.

4. 국제민간항공기구(ICAO)

국제민간항공기구(ICAO)는 국제 테러 위협에 대응하기 위해 국제법을 통하여 여러 가지 상호협력을 위한 노력이 기울여왔다. 여기에는 동경협약(1963년), 헤이그협약(1970년), 몬트리올협약에 대한 부속협약(1988년), 가소성 폭약 표식을 위한 협약(1991년) 등 5개의 항공보안 관련 국제협약(international

convention)이 있다. 우리나라의 경우 이 모든 협약에 가입하였다. 그 동안 우리나라는 별도 법률을 제정하지 않고 협약을 국회 비준을 통하여 국내법과 동일하게 적용해왔다. 그러나 주요사항에 대해서는 항공안전 및 보안에 관한 법률에 포함하여 시행하고 있다.⁴³⁾

1) ICAO 동경협약

동경협약으로 알려져 있는 ‘항공기 내에서 범한 범죄 및 기타 행위에 관한 협약’(Convention on the Offences and Certain Other Acts Committed on Board Aircraft)은 1963년 9월 4일 서명, 1969년 12월 4일 발효되었다.

1950년부터 증가하기 시작한 국제 항공기 납치에 대한 처벌근거가 미약하고 항공기내 범죄 발생시 어느 나라가 관할권을 가지는지를 결정할 필요가 있었다. 이에 따라 1963년 8월 동경에서 개최된 ICAO 회의에서 최초의 국제항공 범죄분야의 다자간협약이 제정되었다. 이 협약을 ‘Crimes Aboard Aircraft Convention’이라고도 부른다.

동경협약은 항공기의 안전과 기내의 인명과 재산, 그리고 민간항공의 안전을 도모하기 위하여 제정되었다. 구체적인 목적은 첫째, 관할권에 관한 규칙의 통일, 둘째, 관할권의 공백을 채우는 문제, 셋째, 기내의 법과 질서의 유지, 넷째, 협약에 따라서 행동하는 사람의 보호, 다섯째, 하기된 사람의 이익보호, 여섯째, 항공기 하이재킹 문제 등을 다루기 위한 것으로 분류된다.

동경협약은 기내 범죄자에 대한 체약국의 처벌의무, 승객·승무원의 안전을 보장하고 피납된 항공기의 무사귀환을 보장하기 위한 최소한의 의무, 항공기 등록국의 공해문제 또는 어느 국가의 영토 이외의 지역에서 비행 중 기내에서 발생한 범죄에 대한 재판 관할권을 제공하도록 규정하였다.

그러나 동경협약은 항공기 납치방지에 상당한 기여를 하였으나 항공기 납치

43) 본 절의 내용은 ICAO 홈페이지(<http://www.icao.int>) ; 김철환, 「항공안전보안개론」, 대왕사, 2004. ; 고광남·소대섭, 「항공보안론」, 백산출판사, 2006. 등을 참조하여 정리함.

에 대한 구체적인 규제, 특히 소추와 처벌에 관해서는 언급되지 않은 것이 미비점으로 지적되고 있다. 또한 기내에 있는 범죄자에 의해 발생된 범죄에만 적용되며 지상에서 범한 행위 또는 범죄는 제외되는 문제점을 갖고 있다.

2) 항공기의 불법납치 억제를 위한 협약

헤이그협약으로 알려져 있는 ‘항공기의 불법납치 억제를 위한 협약’(Convention for the Suppression of Unlawful Seizure of Aircraft ; THE HAGUE CONVENTION 1970)은 1970년 12월 16일 헤이그에서 서명, 1971년 10월 14일 발효하였다.

1968년부터 항공기 납치가 급격히 증가하게 되었는데(<표 3-4>), 이에 대한 대책으로 헤이그협약이 출현하였다. 이 당시 항공기 납치는 주로 정치적 목적을 가진 테러범들의 무차별적이고 비인간적인 범행으로 동경협약만으로는 급증하는 항공기 납치에 대처하는 데 불충분하다는 여론이 있어 이를 보완하기 위해 제정되었다.

헤이그협약은 주요 목적은 동경협약을 보완하고 항공기 납치범에 대한 처벌을 하기 위한 것이다.

〈표 3-4〉 항공테러 발생 현황

구분	파괴행위	납치	납치시도	기내공격	공항시설	기타	계
1970년	13	49	38	-	-	-	100
1971년	3	38	20	-	-	-	61
1972년	13	43	36	-	-	-	92
1973년	12	17	12	-	-	-	41
1974년	20	13	14	-	-	-	47
1975년	24	12	11	-	-	-	47
1976년	28	13	13	-	-	-	54
1977년	31	18	16	-	-	-	65
1978년	11	13	13	-	-	-	37

〈표 3-4〉 항공테러 발생 현황(계속)

구분	파괴행위	납치	납치시도	기내공격	공항시설	기타	계
1979년	11	16	10	-	-	-	37
1980년	8	29	17	-	-	-	54
1981년	15	24	14	-	-	-	53
1982년	6	19	11	-	-	-	36
1983년	7	21	17	-	-	-	45
1984년	13	21	7	-	-	-	41
1985년	13	20	7	-	-	-	40
1986년	3	5	6	-	-	-	14
1987년	3	4	6	-	-	-	13
1988년	2	7	3	-	-	-	12
1989년	2	8	4	-	-	-	14
1990년	-	13	8	1	1	-	23
1991년	-	7	5	2	1	-	15
1992년	-	6	2	1	1	-	10
1993년	-	21	4	2	1	2	30
1994년	2	20	5	3	4	3	37
1995년	-	9	2	1	2	-	14
1996년	-	10	2	-	1	2	15
1997년	-	4	1	-	-	1	6
1998년	-	6	1	-	1	1	9
1999년	-	6	-	-	-	-	6
2000년	-	9	1	1	-	1	12
2001년	-	7	1	-	2	1	11
2002년	-	2	6	1	3	1	13
2003년	4	3	5	3	-	19	34
2004년	3	1	2	-	2	1	9
계	247	514	320	15	19	32	1,147

자료 : ICAO.

헤이그협약은 국제항공에만 적용되는 것이 아니라 국내항공에도 적용되는 것이 특색이다. 범인을 반드시 처벌하여야 하며, 범인을 처벌하지 않는 유일한 방법은 범인을 처벌할 다른 나라에 인도하는 것이다. 헤이그협약은 몬트리올협약과 함께 이 같은 범죄인의 인도의도를 강화하였다.

그러나 헤이그협약은 범인에 대하여 처벌하도록 규정은 하고 있으나, 구체적인 처벌 정도에 대해서는 명시하지 않고 있다. 따라서 특정국가에서 항공기 납치범에 대하여 가벼운 형량으로도 처벌할 수 있다는 문제가 발생한다.

3) 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약

‘민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약’은 몬트리올협약으로도 알려져 있고, 1971년 9월 23일 서명, 1973년 1월 26일 발효하였다.⁴⁴⁾

1970년대 아랍 테러리스트가 자행하는 항공기 폭파사건이 연속적으로 발생하였는데, 동경협약이나 헤이그협약으로는 이러한 테러리스트들을 처벌할 수 없는 문제가 발생하였다. ICAO에서는 이러한 협약을 보완하기 위하여 신 조약의 작성에 착수하여 1971년에 이 협약을 제정하였다. ‘민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약’을 수립하였다.⁴⁵⁾

이 협약의 제정 목적은 항공기 납치범에 대한 처벌뿐 아니라 지상에서의 공격 및 항공시설에 대한 공격 행위를 엄격하게 처벌하기 위한 것이다.

몬트리올협약은 항공기 파괴행위자에 대한 체포, 기소, 추방에 대하여 명시하고 있고, 서명국이 파괴행위자를 위한 대책을 수립하도록 규정하고 있으며, 그러한 행위가 영향을 미칠 수 있는 관련 국가에 통보하도록 명시하고 있다.

그러나 이 협약은 범죄의 정의를 제외하고는 헤이그협약의 유형과 유사하고 실제적으로 동일한 사항이 많다. 공항 및 티켓 카운터에서 발생하는 불법방해 행위에 대한 대응사항이 빠져 있다.

4) 국제 민간항공기 취항공항에서 불법폭력행위 억제 의정서

일반적으로 ICAO 몬트리올협약보충서로 불리는 ‘국제민간항공기 취항하는

44) 우리나라 국회동의일 1973. 6. 2. 가입서 기탁일 1973. 8. 2. 발효일 1973. 9. 11.

45) Convention for Suppression of Unlawful Acts Against the Safety of Civil Aviation

공항에서 불법폭력행위 억제를 위한 의정서⁴⁶⁾는 1988년 2월 24일 몬트리올에서 천명, 1989년 8월 6일 발효하였다.

1985년 12월 27일 발생한 로마 공항과 비엔나공항 동시공격사건⁴⁷⁾ 이후 몬트리올협약에서 간과한 공항 및 티켓 카운터에서 발생하는 불법행위에 대한 대응을 하기 위하여 몬트리올 부속협정으로 1988년 2월 24일 몬트리올에서 서명되었으며 서명국 정부의 권한을 국제공항에서 발생하는 공격통제까지 확대하였다.

이 협약은 공항 및 티켓 카운터에서 발생하는 불법방해행위를 포함한 국제공항에서의 불법행위에 대한 처벌을 위해 제정되었다. 즉 불법적이고 의도적으로 국제공항에서 인명을 다치게 하거나 사망하게 하는 폭력행위와 공항시설 또는 운항 중에 있지 아니한 항공기에 위해를 가하여 공항에서의 안전을 위협하는 파괴행위 등에 대하여 처벌하기 위하여 제정된 것이 특징이다.

5) 탐지목적의 플라스틱 폭발물 표시에 관한 협약

이 협약⁴⁸⁾은 1991년 3월 1일 몬트리올에서 승인되었고, ‘ICAO 가소성 협약’이라고도 부른다. 이 협약은 각국에서 무분별하게 폭발물을 제조·사용하여 공항에서 이러한 폭발물 탐지가 어려워짐에 따라 이를 통제하기 위하여 제정되었다. 즉 각 국가에서 생산하는 폭발물이 공항검색에서 쉽게 발견될 수 있도록 통제하기 위하여 제정되었다.

ICAO 가소성 협약은 테러리스트의 플라스틱 폭발물 위협에 대응하기 위하

46) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation 1988

47) 로마 및 비엔나 공항 동시공격 사건은 대표적인 공항시설 공격사건으로 기록된다. 1985년 12월 27일 로마공항 및 비엔나 공항에 아부니달 테러분자가 탑승수속을 받고 있는 승객에게 수류탄 투척 및 자동소총을 무차별 난사하여 15명을 사망시키고 70명을 부상시키는 대규모 공항공격사건이 발생하였다. 공항 동시 공격사건이고 고의적으로 어린이를 대상으로 공격하여 피해를 많이 일으킨 사건이다(김철환, 전게서, pp. 38~39).

48) Convention on the Marking of Plastic Explosives for the Purpose of Identification.

여 폭발물 제조시 공항에서 쉽게 탐지할 수 있도록 특수약품을 삽입하도록 하고, 폭발물 소유 및 운송에 엄격한 통제를 실시토록 하며, 기존에 확인할 수 없는 폭발물을 가능한 전량 파기하도록 하는 내용을 포함하고 있다.

6) 국제민간항공협약 부속서17 항공보안 규정

항공보안에 대한 국제민간항공기구(ICAO)의 정책방향은 국제민간항공협약⁴⁹⁾의 부속서 17(ANNEX 17) 항공보안(Aviation Security)에 잘 나타나 있다.

부속서 17은 국제민간항공에서의 폭력범죄가 지속적으로 증가하자 항공기 납치와 같은 불법행위에 관한 문제를 규정하기 위하여 1972년 항공보안 대책이 최초로 제안되었으며, 관련 체약국의 의견과 이사회의 의견을 수렴하여 1974년 3월 22일 이사회에 의해 최초로 민간항공협약에 대한 부속문서로 ICAO 시카고협약부속서 17(항공보안)이 제정되었다. 1975년 2월 27일부터 적용되고 있다. 현재 부속서 17은 10차례 개정되었고, 가장 최근 판은 2001년 12월 7일 채택되었으며 2002년 7월 1일부로 적용되고 있다. 이 부속서는 국제민간항공산업의 항공보안기본규정으로 정착되었다.

부속서 17의 해당항목에는 각 체약국은 자국 민간항공 보안계획의 목적이 불법행위로부터 민간항공을 보호하는 규정·세칙·절차를 통해 국제민간항공의 효율성과 안전성을 확보하도록 규정하고 있다. 부속서 구성은 표준지침과 권고안 2가지 형태로 구분된다.

표준지침(standard)은 원문에는 ‘shall’로 표현되고 있으며, 물질적 특성과 형상, 시설, 성능, 종사자, 절차 등에 관한 세칙으로 통일적 적용이 국제항공의 안전성과 정확성을 확보하기 위한 것으로 각 체약국이 반드시 준수하여야 한다. 만약 이를 준수하지 못할 경우 시카고 협약 38조에 의거하여 각 체약국의 대안으로 수행하는 해당방식을 ICAO에 통보하도록 되어 있다. ICAO는 이를

49) Convention on International Civil Aviation.

접수하여 상이점에 대해 부속서 17의 첨부 형태로 각 체약국에 배포하고 있다.

권고안은 원문에는 ‘should’로 표현되고 있으며, 국제적 통일적용이 인정되거나 각 체약국이 반드시 준수하여야 하는 사항은 아니지만 준수토록 노력해야 하는 규정이다. ICAO 부속서 17 중에서 공항과 관련하여 포함하도록 권고하는 내용은, i) 항공보안관련 각 담당기관별 명확한 책임 분장, ii) 공안보안위원회 설치, iii) 보안관련 정보 및 연락체계 마련, iv) 공항 경비 보안대책, v) 불법 방해 행위에 대한 대응, vi) 보안교육훈련, vii) 기타 공항조직도, 에어 사이드와 랜드 사이드를 구분하여 표시한 요도, 터미널 지역 배치도, 보안구역별로 표시한 배치도, 관련 법규 등이다. 현재 우리나라는 ICAO 부속서 체약국으로, 부속서의 내용은 국내법과 동일한 효력을 갖고 있다.

7) ICAO 항공보안지침서 문서 8973/6⁵⁰⁾

이 지침은 각 체약국이 부속서 17의 항공보안사항을 적절히 시행할 수 있도록 지원하기 위하여 ICAO 사무국과 5개국 전문가로 구성된 자문그룹에서 작성하여 1971년 최초로 발간되었다. 2002년 12월에 6판까지 발행되어 있다.

이 지침은 각 체약국이 ICAO 부속서 17의 표준지침 및 권고안에 대한 시행을 위한 가이드로 ICAO 부속서 17의 관련 항목별 상세한 지침을 수록하는 형태로 되어 있다. 주요내용사항은 모든 항공보안관련 지침 및 절차에 대한 상세사항을 포함하고 있다. 배포제한 대외비 문서로 분류하고 관련기관에 한정적으로 배포하고 있다.

8) 시사점

국제민간항공기구의 반테러 활동은 1960년대부터 시작되어 역사도 오래되

50) 불법행위로부터 민간항공보호를 위한 보안지침서.

있고 시스템도 잘 갖추어져 있는 것으로 평가된다. 그리고 ICAO 협약의 각국 수용실태도 대체로 양호하여 다른 물류부문에서 활용도도 높은 편이다. 국제민간항공기구의 보안관련 협약을 비롯한 일련의 활동에서 시사하는 바를 정리한다.

첫째, ICAO 물류보안관련 협약의 계속적 강화에 준비해야 한다. ICAO 보안관련 협약은 1969년 발효된 동경협약으로부터 시작되어 최근 ICAO 항공보안지침서 문서 8973/6(불법행위로부터 민간항공보호를 위한 보안지침서)까지 대상범위와 처벌규정, 각국의 의무조항 등이 계속 강화되고 확대되고 있다. 이에 따라 국내 민간 항공사뿐만 아니라 항공 포워드, 항공화물 하주 등의 부담이 증가할 수밖에 없다. 그리고 정부기관의 책임과 역할도 강화되고 있다. 따라서 우리나라가 급증하는 항공화물을 적절히 처리하고 동북아 물류 중심화를 위한 정책을 지속적으로 추진하기 위해서는 항공화물의 보안시스템도 국제기준에 부합되도록 완비하고 더 나아가 이를 적절히 활용하는 전략도 마련해야 한다. 즉 “인천국제공항=안전한 공항”이라는 브랜드화가 필요한 시점이다.

둘째, ICAO 부속서 규정의 국내 항공 적용에 대비해야 한다. 개정된 부속서 17의 경우 국내항공활동에도 국제항공에 적용되는 표준을 적용할 것을 의무화하고 있어 이제는 부속서 17의 내용을 국내 항공활동에도 적용해야 한다. 이는 9·11 테러가 국내선을 대상으로 자행되었기 때문이다. 따라서 우리나라도 국내 항공 활동에 대해 부속서 17의 규정을 준수해야 하는데, 민간 항공사의 경우 국제항공활동을 통해 이미 이 내용을 수용하고 있기 때문에 별다른 어려움이 없다. 그러나 지방 공항과 항공관련 행정기관, 보안관련 기관들이 이에 대해 정확히 이해하고 수용해야 하는 과제가 남아 있다.

셋째, 항공 테러에 대비한 정부의 역할과 책임이 강화되어야 한다. 국제민간항공기구(ICAO)의 항공보안 프로그램에서는 회원국 정부가 자국의 항공 보안 전반에 대한 책임이 있음을 분명히 하고 있다. 이에 따라 미국 등 일부 국가에서는 정부가 직접 항공 보안활동을 수행하고 책임을 지고 있다. 즉 미국은 화물의 보안은 항공사가 지도록 하고, 여객안전은 국가가 책임지도록 분담을 하

고 있다. 더 나아가 미국은 화물 보안도 정부에서 직접 통제하려는 움직임을 보이고 있다. 반면 우리나라의 경우 승객이나 수하물의 보안검색, 공항의 보안 구역 설정 및 운영 등은 공항공사가 책임지도록 되어 있고, 화물 보안과 항공기에 대한 보안 업무는 항공사가 책임지고 수행하도록 되어 있다. 따라서 우리나라 정부도 항공 보안에 대해 행정적인 지도를 넘어 보안제도 및 보안 시스템과 장비를 확보하고 구축하는 일에 인력과 예산을 확대해야 한다.

넷째, 항공물류보안의 표준화에 대비해야 한다. 국제민간항공기구의 부속서 17 및 항공보안지침서 문서 8973/6은 민간항공을 보호하기 위해, 협약의 체결국은 자국 민간항공 보안계획의 목적이 불법행위로부터 민간 항공의 안정성과 효율성을 확보하도록 규정하고 있다. 특히 ICAO 부속서 17의 표준 지침은 각국의 반드시 준수해야 하는 바 향후 이에 대한 내용이 표준화 될 가능성이 높다. 즉 항공보안 확보항공화물의 안전성 제고를 위한 방안으로 위험물 검사방법, 기술, 장비, 시스템이 표준화될 가능성이 높다. 더 나아가 항공화물 검사에 필요한 장비나 시스템을 사용할 때 특정 기술이 활용된 경우로 한정하는 경우가 발생할 수 있어 이에 대한 정부 및 업계의 대책이 필요하다.

제4장

주요국의 물류보안 정책과 시사점

1. 미국의 물류보안제도

1) 국토안보부(DHS) 신설

2001년 9·11 테러 이후 미국은 향후 예상되는 테러리즘으로부터 국토를 보호하고, 국경을 통제하는 첫 번째 조치로 보안 관련 행정조직을 일원화하였다. 미국은 자체적으로 시행한 보안 평가와 의회 청문회 등을 통해 얻은 증언 등을 토대로 행정조직을 개편하기로 하고, 이에 대한 대책의 하나로 2003년 1월 국토 안보부(Department of Homeland Security, DHS)를 설치하였다.⁵¹⁾

국토 보안부 신설은 지금까지 22개 정부부처에 분산·집행되고 있던 국경 통제와 보안 업무를 일원화하는 것으로, 2003년을 기준으로 공무원 수가 17만 명, 예산 374억 달러가 넘는 초대형 정부 부처로 부상하였다. 당초 미 정부는 재무부의 일부 기능과 CIA의 기능도 이 조직에 포함시키는 방안을 검토하였으나 의회 입법 심의 과정에서 반대에 부딪쳐 현재의 조직으로 최종 확정되었다.

국토 안보부는 테러로부터 미국을 지키는 최고 기관으로 주로 다음과 같은 업무를 수행하고 있다. 즉, i) 국경 및 운송 수단의 보안조치, ii) 비상사태에 대한 대응조치 강구, iii) 화학무기 및 핵무기 사용 대응조치, iv) 정보 분석 및

51) 국토안보부는 부시 대통령이 의회의 의결을 거쳐 행정부로 이송된 국토안보부 설립에 관한 법률(HR 5005)에 최종 승인함에 따라 설립절차를 마쳤음.

기간 시설 보호 등에 관한 업무를 수행하고 있는데, 이 같은 업무를 효율적으로 처리하기 위하여 연안경비대(USCG)와 관세청(CBP)의 기능을 통합한 것은 물론 중앙정보국(CIA)과 연방수사국(FBI), 연방 비상 관리청의 기능도 일부 이관 받은 매머드 조직이다.⁵²⁾

국토 안보부 출범과 함께 그 동안 다른 기관에 소속되어 있던 미국 연안경비대, 교통안전청(Transportation Security Administration)과 이민·귀화국(Immigration and Naturalization Service)도 3월 1일부터 이 부처에 통합되었다. 당시 톰리지(Tom Ridge) 국토 안보부 장관은 교통부(DOT)에서 연안경비대 업무를 이관 받음에 따라 이 부서의 군사·해사 관련 업무가 국토안보부의 주 기능이 될 것이라고 밝혔다.

또한 같은 교통부 소속이었던 교통안전청은 국토안보부로 이관되면서 인력을 6만 4,000명으로 증원하였으며, 항공기 승객 및 화물에 대한 검색 업무를 주로 담당하고 있다. 이민·귀화국은 국토안보부로 통합된 이후 망명자 및 난민 처리, 미국 내 거주 외국인 관리업무 및 귀화 관련 업무를 담당하게 된다. 이와 같은 부처 통합 조치는 그 동안 교통부 등 여러 부서에 나뉘어져 있던 보안 관련 업무를 한 곳으로 통합함으로써 체계적인 보안관리체계를 갖추기 위한 미국의 새로운 물류보안 통합조치로 인식되고 있다.⁵³⁾

이 부서는 설립 이후 ‘국토 안보부 대통령 지침 7’⁵⁴⁾에 따라 테러를 차단하는데 필요한 기본적인 전략을 마련한 뒤 철도 및 운송 보안 지침, 국가 해운보안대책 등을 수립, 물류 보안 확립에 최선을 다하는 한편, 2006년 6월에는 국가 사회간접자본 보호 계획⁵⁵⁾을 마련하였다.

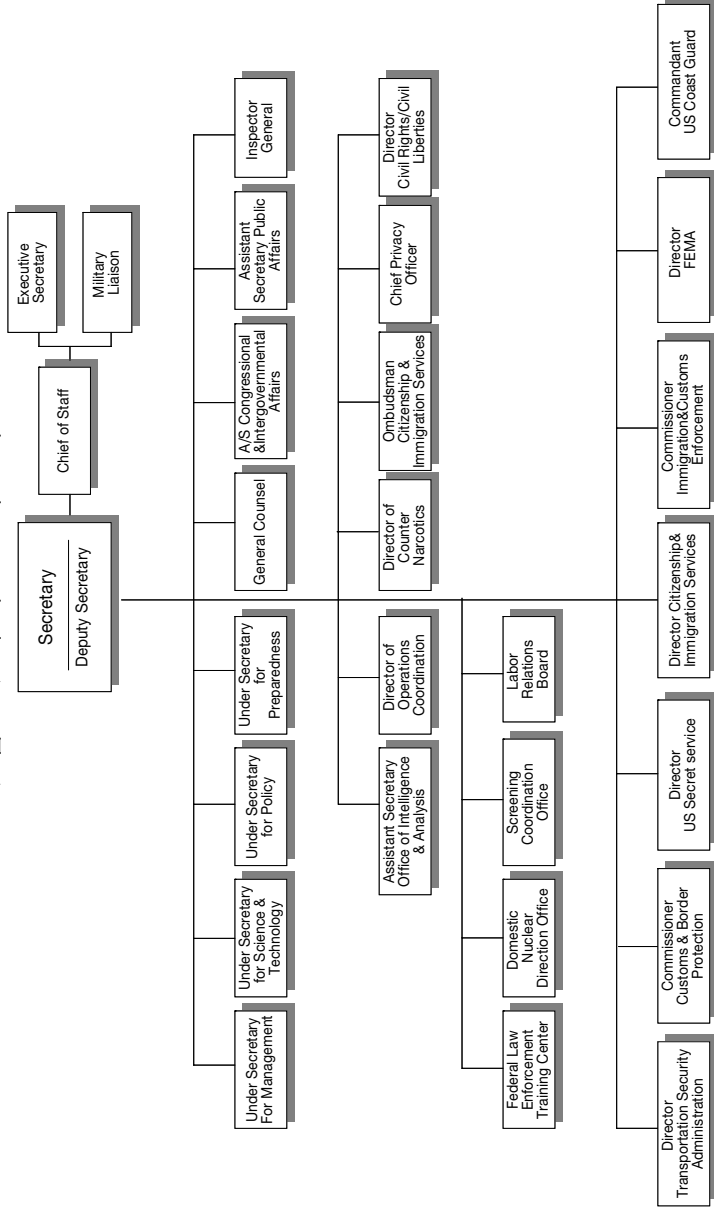
52) 국토 안보부는 출범 이후 자체적으로 수립한 국가안보 기본 전략(National Strategy for Homeland Security)에서 국토 안보의 목적에 대해, 1) 미국 내에서 테러 공격의 방지, 2) 테러 취약점 감소, 3) 테러 공격이 일어난 경우에 피해 최소화와 복구 등이라고 밝히고 있음. 이 같은 임무는 2002년의 국토 안보부 설립에 관한 법률(제101조)의 규정과 동일함.

53) *American Shipper*, 2003. 2. 28

54) Homeland Security Presidential Directive 7

55) National Infrastructure Protection Plan, 2006. 6

〈그림 4-1〉 미 국토 안보부 조직도



2) 컨테이너 보안협정 시행

미국은 자국으로 대량살상무기(Weapons of Mass Destruction, WMD) 등이 밀반입되는 것을 차단하기 위해 2002년 1월부터 컨테이너 보안 협정제도(Container Security Initiative, CSI)⁵⁶⁾를 마련하여 시행하고 있다. 이 제도의 핵심은 미국과 미국인의 인명과 재산을 해할 수 있는 무기 등 테러에 사용되는 물품이 선박을 통하여 미국에 몰래 반입되는 것을 막는 데 있다. 미 관세청장은 2002년 1월 “미국은 지금 위험한 화물이 도착할 때까지 앉아서 기다릴 시간적 여유가 없다”고 강조하면서 외국 항만에서 미국행 화물이 선박에 적재되기 전에 검사를 시행하여야 하고, 그 화물과 선박에 대한 모든 정보를 미국 입항 전에 전자적인 방법으로 제공받아 분석할 방침이라고 밝혔다.⁵⁷⁾

이 제도의 주요내용은 i) 외국항만에서 미국 관세청 검사관과 해당국가의 관련 기관이 ii) 미국으로 수출되는 컨테이너 화물을 대상으로 iii) 그 화물이 선박에 적재되기 전에 iv) 위험성이 있는지 여부를 방사능 탐지기나 화물 투시기(X-ray)와 같은 기계적 장비로 검사하여 v) 위험화물로 판단되는 경우 미국 입항을 금지하는 등 적절한 조치를 취하도록 되어 있다.

미국은 컨테이너 보안 협정의 적용대상으로 미국행 화물을 대량으로 선적하는 세계 20대 항만(mega port)을 우선 선정하였다. 제도 도입 초기인 2003년 1월 25일 현재 대상항만 거의 대부분이 이 제도를 시행하기로 미국과 양자협정을 체결하였거나 시행한다는 원칙에 합의하였다. 이 협정을 체결한 국가는 전 세계 주요 항만국을 포함하고 있으며, 이들 항만에서 미국으로 수출되는 컨테이너 화물량은 미국 전체 수입물량의 68%를 차지하고 있다.

유럽에서는 독일, 네덜란드, 프랑스, 영국 등이 이에 포함되어 있다. 아시아권에서는 중국, 일본, 싱가포르, 홍콩, 우리나라 등이 참여하고 있다. 우리나라

56) 이 용어는 현재 각각 달리 번역되어 사용되고 있는데, 우리나라 관세청에서는 컨테이너 안전대책으로 지칭하고 있음. 이 글에서는 이 제도가 안전(safety)보다는 보안(security)을 강조하고 있는 점을 고려하여 컨테이너 보안협정으로 사용함.

57) 최재선, “미국, 외국 컨테이너 화물 보안검사제도 시행”, 『해양수산동향』, 한국해양수산개발원, 2003. 1. 27.

는 2003년에 서울에서 미국과 협정을 체결하였다. 이에 앞서 우리나라는 2003년 9월 관세청장이 미국을 방문하여 이 제도를 국내 부산항에서 시행하기로 잠정적으로 합의하였으며, 그 동안 미국 관세청 직원이 주재하는 문제와 구체적인 시행방안 등에 대해 의견을 교환해왔다.⁵⁸⁾ 양국 합의에 따라 우리나라는 부산항을 단순 경유하는 화물을 제외한 모든 미국행 컨테이너 화물을 검사하고, 위반사실이 발견될 때는 우리나라 법률에 따라 처리하도록 명문화되었다.

〈표 4-1〉 CSI 시행 항만 및 미 입항 물동량

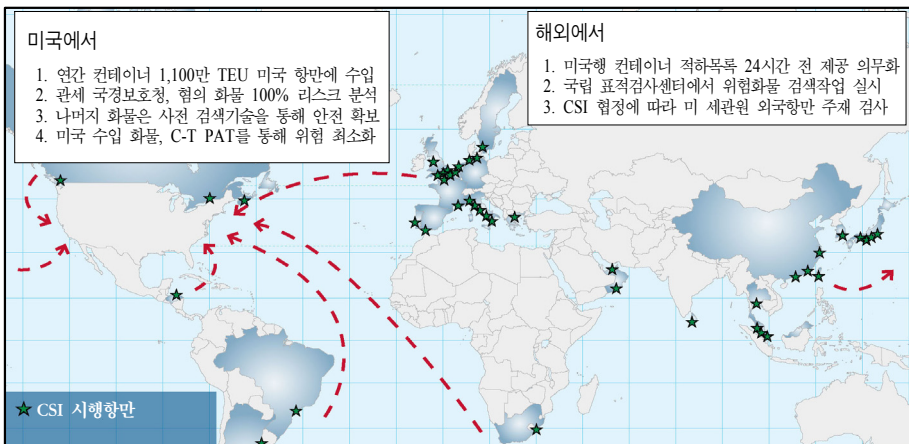
항만	2005년 물동량(TEU)	항만	2005년 물동량(TEU)
Yantian(Shenzhen)	2,342.38	Gioia Tauro	96.14
Hong Kong	1,866.14	Livorno(Leghorn)	96.02
Shanghai	1,696.41	Felixstowe	73.70
Kaohsiung	1,154.69	Algeciras	60.35
Busan	1,121.67	Buenos Aires	54.88
Singapore	534.56	Liverpool	43.42
Rotterdam	457.32	Tanjung Pelepas	43.25
Bremerhaven	432.68	Durban	42.26
Antwerp	317.80	Port Kelang	40.42
Tokyo	288.77	Thamesport	33.36
Nagoya	187.92	Naples	33.19
Leam Chabang	178.38	Southampton	32.35
Cortes	172.8	Lisbon	22.90
Le Spezia	158.42	Halifax	22.86
Hamburg	158.41	Göteborg	19.13
Santos	155.70	Piraeus	10.18
Salalah(Oman)	129.60	Vancouver	8.99
Kobe	129.50	Tibury	2.92
Genoa	122.87	Dubai	0.98
Yokohama	122.74	Marseille	0.69
Le Havre	120.83	Montreal	0.17
Colombo	114.30	Zeebrugge	0.04
CSI 항만 합계		12,702.09	
비 CSI 항만 합계		4,588.26	
전체 항만 합계		17,290.35	

자료 : 미국 세관 · 국경보호국

58) 미국과 CSI를 체결한 우리나라의 경우 미국 CBP 직원 3명을 부산에 상주시키면서 미국행 수출 컨테이너 화물을 검사하는 데 활용하고 있음.

이 제도가 시행된 지 5년이 지난 2006년 6월 현재 적용대상 항만이 크게 늘어났다. 제도를 시행하고 있는 미국 세관·국경보호국의 지속적인 노력에 힘입어 CSI에 가입한 국가는 북미와 유럽, 아시아, 아프리카, 중동 및 중남미 등 26개 세관 당국과 협정을 맺었다. 미국은 2006년 회계연도 말까지 CSI 시행하는 항만을 50곳으로 확대할 방침인데, 이렇게 될 경우 태평양과 대서양 등을 통해 미국으로 수출되는 컨테이너 화물의 90%가 외국의 선적 항만에서 사전 검색을 받게 된다.

〈그림 4-2〉 CSI 처리 절차



● 헬리팩스(몬트리얼, 밴쿠버(캐나다))	● 앤트워프(벨기에)	● 펠릭스토우(영국)	● 나폴리(이탈리아)	● 알제시라스(스페인)	● 카오슝(중국)
● 로테르담(네덜란드)	● 지브르(벨기에)	● 리버풀, 템즈포트, 티버리, 사우샘프턴(영국)	● 지오이아 타오르(이탈리아)	● 나고야, 고베(일본)	● 산토스(브라질)
● 리 하브르(프랑스)	● 싱가포르	● 제노아(이탈리아)	● 부산(한국)	● 램차방(타이완)	● 콜롬보(스리랑카)
● 마르세이유(프랑스)	● 요코하마(일본)	● 라스페차(이탈리아)	● 다반, 남아프리카	● 두바이, 아랍에미리트(UAE)	● 브레노스아이레스(아르헨티나)
● 브레메해븐(독일)	● 홍콩	● 라스페차(이탈리아)	● 포트클랑(말레이시아)	● 리스본(포르투갈)	● 포트 사라하(오만)
● 함부르크(독일)	● 고텐베르크(스웨덴)	● 리보르노(이탈리아)	● 탄중펠레파스(말레이시아)	● 상하이(중국)	● 코르테스(온두라스)
			● 피라에우스(그리스)	● 선전(중국)	

자료 : 한국해양수산개발원

2006년 6월 들어 미국은 중동의 오만과 이집트, 그리고 중남미의 온두라스와 자마йка 등과 CSI 협정을 체결하는 등 발 빠르게 움직이고 있다. 현재 미국과 CSI 협정을 맺고, 컨테이너 화물에 대한 검사를 시행하고 있는 항만은

모두 44개로, 미국 수출 화물의 75%를 점유하고 있다.⁵⁹⁾ 미국은 개별국가와 협정을 체결, 이 제도를 시행하는데 그치지 않고, 세계세관기구(WCO)와 경제협력 개발기구(OECD) 등을 통해 세계적인 확산을 도모하고 있다.

3) 화물정보 선적 24시간 전 신고제도

미 세관 · 국경보호국은 CSI제도를 보완하는 조치의 하나로 이른바 ‘24시간 규칙’을 도입하여 시행하고 있다. 이 제도는 미국으로 컨테이너 화물을 수출하는 모든 운송인에게 화물을 선박에 적재하기 24시간 전에 적하목록을 CBP의 자동 적하목록 시스템(Automated Manifest System)에 신고하도록 하는 것을 핵심으로 하고 있다.

〈표 4-2〉 미 관세청 24시간 규칙의 주요내용

구분	주요내용
화주의 의무	○ 선사에게 정확한 선적 화물정보(15개 항목) 제공
선사의 의무	○ 화물 선적 24시간 전 화물정보 미 관세청에 신고 ○ 미국항만에 양륙하지 않는 화물정보도 동시 신고
위반시 책임	○ 당해 화물의 미국항만 양륙 허가 불허 ○ 위반하는 경우 5,000달러 벌금(위반건수 당) ○ 대량살상 무기등이 선적된 경우 선박 억류 및 몰수
선화주 대책	○ 화주 : 1) 선적 72시간 전에 화물정보 선사 제공 2) 출항 24시간 전에 해당화물 항만 반입 ○ 선사 : 1) 화물선적 24시간 전에 미 관세청에 신고 2) 선적마감시간 고려 화물 선적계획 작성
신고시 주의사항	○ 화물 정보 기재 명확화 : FAK, Consolidated Cargo, Said to Contain 등 표현 사용 금지 및 화물 수량의 수치 정확하게 해야 함

자료 : 한국해양수산개발원

59) JOC, 2006. 6. 23

이 제도는 현행 컨테이너보안 협정(CSI)과 표리관계에 있는 것으로, 외국 항만에 파견되어 있는 미국 세관원에게 검사대상화물에 대한 정보를 즉시 제공하는 효과 외에 외국 항만에서 시행된 컨테이너 보안 검사에서 적발되지 않은 미국행 화물을 미국 항만에서 다시 검사할 수 있는 이중 검색 수단으로 활용하려는 데 제도의 목적이 있다.

이 같은 신고 규정을 위반하는 경우 해당 화물 선적하고 입항한 선장에게 첫 위반에 대해서는 5천 달러, 그 이후의 위반에 대해서는 위반시마다 1만 달러의 벌금과 함께 선박을 억류하거나 몰수할 수 있는 처벌 규정도 아울러 두고 있다.

4) 민·관 협력 반테러 보안제도

미국이 역점을 두고 시행하는 또 다른 제도의 하나는 지난 2001년 11월에 처음으로 도입한 뒤 2002년 4월부터 본격적으로 시작한 이른바 ‘반테러 세관-무역업자 간 파트너십(C-T PAT : Customs-Trade Partnership Against Terrorism) 프로그램이다. 이 제도는 미국으로 화물을 수출하는 모든 제조업자, 화주, 선사 등에게 화물의 공급사슬 전반에 걸쳐 보안성을 확보하도록 하는 것으로 관세청이 민간기업과의 협정을 통하여 시행하고 있다.⁶⁰⁾

화주 등이 이 프로그램에 가입하기 위해서는 관세청에서 사전에 만든 보안 지침에 따라 자체 시설 및 인원 등에 대한 보안성을 평가한 뒤 가입 신청서를 제출하고, 미국의 평가와 승인을 받아야 회원 자격이 부여된다. 미국은 이 제도 도입 초기에는 일부 대형 화주나 선사 등에게만 제한적으로 적용하였으나, 지난 7월부터는 미국 수출관련 모든 업체에서 가입할 수 있도록 개방하였다.

60) 이 프로그램에 참여할 수 있는 업종으로는 미국 수입업자, 선사 및 항공사, 항만 터미널 운영업체, 도로운송사업자, 혼재업자, 포워더(화물운송 주선업자), 통관중개인 등이며, 외국의 제조업체도 일부 참여하고 있음. 미국은 이 제도를 자발적인 차원에서 시행하고 있으나 미국의 수입업체에 대해 이 제도 가입을 허용함에 따라 실질적으로는 외국의 제조업체도 이 제도를 강제적으로 이행하여야 하는 환경이 조성된 것으로 전문가들은 보고 있음.

C-T PAT 회원 자격을 신청하기 위해서는 적용대상 별로 CBP가 설정한 최소한의 물류 보안 기준(시설 및 인력의 보안 담보, 운송보안 및 화물 추적 등)을 이행하고 있어야 하는데, 미국은 각 업종별로 지켜야 하는 최소한의 보안 기준을 별도로 제정하여 시행하고 있다.

미 세관·국경보호국은 이 제도에 참여하는 업체의 경우 화물유통과정에서 안전한 공급 사슬을 보장받을 수 있고, 세관의 통관검사 감소로 고객 서비스를 향상시킬 수 있는 이점이 있다고 강조하고 있다. 특히 미국은 가입 회원에 대한 등급을 3단계로 구분하여 다음과 같이 각각 차별화된 혜택을 부여하고 있다.

- 1단계 : 프로그램 참여 허용, 평가 팀의 평가 미완료, 화물 검사 횟수 축소
- 2단계 : CBP 평가 완료업체, 1단계 혜택 외에 화물 우선검사 부여
- 3단계 : 미국 수출화물의 무 검사 통관혜택 부여 및 화물 신속 처리 보장 등이 그것이다.

한편, 이 프로그램에는 2006년 3월 5일 현재 포드와 제너럴 모터스와 같은 대형 제조업체 등 1만 343개 이상의 회사가 가입을 신청하였으며, 전 세계 5,777개 업체가 인증 파트너로 등록되어 있다(외국 제조업체 248사 포함). 미국은 최근 들어 이 제도를 강제화하는 방안을 검토하고 있으나 일부 업체들의 반발이 거세 입법화되기까지는 어느 정도 시간이 걸릴 것으로 보인다.

5) 해운보안법 제정·시행

미국 의회에는 9·11 테러 참사 이후, 해사보안과 관련된 여러 가지 법률안이 제출되어 일부 법률로 확정되었다. 이 같은 법률 가운데, 가장 대표적인 법률인 IMO의 ISPS 코드와 유사한 미국의 해운보안법이다. 이 법률은 미국 항만 및 선박의 보안을 강화하는 내용과 미국에 화물을 수출하는 외국항만이 테러를 방지하는데 필요한 적절한 보안조치를 시행하고 있는지 여부를 평가하고, 시정을 권고하는 사항을 담고 있는 것이 특징이다. 미국 해운보안법의 주요 내

용을 살펴보면 다음과 같다.

첫째, 항만과 선박의 보안취약성 평가를 강제하고 있다. 이는 선박을 이용한 테러 등 운송보안사고⁶¹⁾를 일으키기 쉬운 선박의 종류와 항만을 가려내기 위한 것이다. 미국 해운보안법은 매 5년마다 기초평가를 우선 시행한 다음 이를 토대로 정밀평가를 시행하도록 요구하고 있다. 다만, 정밀평가를 시행하는 데 있어서는 항만시설에 대한 평가보다는 선박의 의한 위협 여부를 판단하는 데 중점을 두도록 한 것이 특징이다.

둘째, 해운보안계획의 수립을 의무화하고 있다. 미국 해운보안법은 이 같은 계획을 크게 두 가지로 나누고 있다. 정부차원에서 수립하는 국가해운보안계획과 이를 토대로 한 지역보안계획, 그리고 각 선박과 항만시설에 따라 작성되는 개별적인 보안계획이 그것이다. 작성된 보안계획은 국토 안보부 장관의 사전승인을 받아야만 시행할 수 있으며, 중요사항이 변경될 때 역시 그러하다.

이 밖에도 이 법률은 해운보안사고에 대한 대응계획의 수립과 보안구역으로 지정된 곳의 출입을 통제하는 운송보안카드제도의 도입, 선박자동식별장치(AIS)의 설치를 의무화하고 있을 뿐 아니라 위성통신기술이나 조난선박구조 및 해상안전시스템(GMDSS⁶²⁾)을 이용한 광대역 선박위치 추적시스템을 개발하고, 입항선박에 대해 화물 정보를 사전에 신고하도록 규정하고 있다.

이 같은 규정은 2004년 7월부터 시행되는 국제해사기구의 국제선박·항만 시설보안 규정(ISPS Code)과 내용 면에서 큰 차이가 없다.⁶³⁾ 이런 점 때문에 미국은 해운보안법과 ISPS Code를 통합·운영하는 방안을 모색하고 있기도 하다. 그러나 이 법률에서 명시하고 있는 외국항만에 대한 보안평가제도는 IMO 제도와는 전혀 판판이다. 미국이 자체적으로 만들어낸 규정이기 때문이

61) 운송보안사고(transportation security incident)라 함은 심각한 인명의 손실, 환경훼손, 운송시스템의 마비 또는 특정지역의 경제적인 혼란을 초래하는 보안 사고를 의미함.

62) Global Marine Distress and Safety System의 약자임.

63) 미국 해운보안법은 선사 및 항만시설 운영자가 이 같은 계획을 수립하는 시기에 대해 이 법률을 시행하는 데 필요한 임시 최종 규칙(interim final regulation)이 제정된 날로부터 6개월 이내라고 정하고 있음.

〈표 4-3〉 미국 해운보안법의 내용

조문		주요내용
제102절	70101	제701장(항만 보안)에서 사용되는 용어의 정의 - 지역해운보안계획, 시설, 선박소유자 및 선박운항자, 해운보안사고 등의 개념 등을 설명하고 있음
	70102	미국 항만시설 및 선박의 보안 취약성의 평가에 관한 규정 - 최초평가(initial assesment)와 정밀평가의 시행에 관한 사항 규정
	70103	해운보안계획의 수립과 시행 - 국가해운보안계획의 수립, 이를 근거로 한 지역해운보안계획, 선박 및 항만시설보안계획의 수립절차에 관한 사항
	70104	해운보안사고에 대한 대응계획의 수립과 시행에 관한 사항 명시
	70105	운송보안카드의 발급절차에 관한 사항
	70106	해상안전 및 보안팀의 설치·운영에 관한 사항
	70107	해운보안분야의 연구를 활성화하는데 필요한 연구개발사업의 진행
	70108	외국항만에서 시행하고 있는 보안제도의 유효성에 대한 평가
	70109	제70108조에 따라 시행된 평가결과의 통보에 관한 사항
	70110	외국항만이 효과적인 반테러조치를 취하지 않고 있는 경우의 대응조치
	70111	선원의 신분확인제도를 보완하는 조치
	70112	해사보안자문위원회의 설립 및 운영에 관한 사항
	70113	해사관련 정보의 수집과 분석에 관한 사항
	70114	선박자동식별장치(AIS)설치 의무화와 선박별 설치시기에 관한 사항
	70115	광대역 선박 추적시스템의 개발과 운용에 관한 사항
	70116	완벽한 운송보안시스템을 구축하기 위한 프로그램의 개발과 시행
	70117	해운보안법의 규정을 위반한 경우의 처벌 규정 - 각 위반마다 2만 5,000 달러 이하의 벌금부과
제103절		국제선원신분증명제도를 강화하는 국제회의의 제안 및 참여
제108절		미국 수출입화물에 대한 정보의 사전 제공과 무서류 화물에 대한 처리
제112절		외국선박에 대한 보고제도
제423절		외국선박이 관련된 해양사고의 조사

자료 : 한국해양수산개발원

다. 이 법률에서 미국은 크게 3가지 점을 염두에 두고 있으나, 미국에 화물을 수출하는 외국항만의 보안상태를 직접 평가한다는 방침이다.

즉, 미국 해운보안법은 국토 안보부 장관에게 미국으로 항해하는 선박이 출항하는 외국항만이 시행하고 있는 반테러조치의 실효성을 판단하여 적절한 조치를 취할 것을 명시하고 있다. 이에 덧붙여 해운보안법은 미국으로 출항하는 선박이 이용하는 항만이 아닌 경우에도 그 항만에서 발생할 수 있는 보안위협이 국제 해운거래에 부담을 줄 것으로 우려되는 경우 동일한 조치를 할 수 있는 권한을 부여하고 있다. 다시 말하면 미국은 해운보안법을 통하여 사실상 외국의 모든 항만에 대해 보안조치의 시행여부와 그 효과의 적절성을 따질 수 있는 근거를 자국법에 둔 것이다.

〈표 4-4〉 미국 및 국제기구의 물류 보안 제도

구분		주요 내용	도입 · 시행
미국	행정부	○ 국가보안부 설치 등 행정 조직 개편 - 연안경비대 등 통합, 인원 17만명	2003년 1월
	관세청	○ 컨테이너 보안 대책(CSI)제도 도입 - 세계 20대 항만 화물 검색 강화	2002년 1월
		○ 반테러 민-관 파트너십(C-TPAT)제도 - 제품의 공급사슬 보안관리시스템	2002년 4월
		○ 적하목록 24시간 사전 신고제도 도입 - 관세청 규칙 개정, 모든 선사 적용	시행
	연 안 경비대	○ 여객선에 화물 탐지기 · 보안요원배치 - 규정 위반 선사에 입항 금지 조치	2002년 7월
		○ 해군 · 연안경비대 합정 보안지역 지정	2001년 10월
		○ 96시간 전 선박 입항 예정시간 통보제	
	국무부	○ 선원의 미국 항만 입국 요건 강화 - 선원의 항만 비자 명부 삭제	2003년 1월
		○ 테러 가능성 선원의 선내 역류 제도 - 미국 다른 항만으로 확대 · 적용	2002년
	법무부	○ 국가 보안 출입관리제도 도입 - 미국 방문자의 지문 날인제도	항만 입국선원 우선적용
	의 회	○ 해운 보안법 제정 및 항만보안법 제정	시행

〈표 4-4〉 미국 및 국제기구의 물류 보안 제도(계속)

구분		주요 내용	도입 · 시행
IMO	법 률 위원회	○ 2005년 항해안전협약 개정 - 범죄인의 소추 및 외국 인도 가능	2005년 10월 제정
	해 사 안 전 위원회	○ 국제 선박 및 항만 보안 규칙 제정 - 1974년 해사인명안전협약 개정	2002년 12월 채택
	총 회	○ 해사 테러리즘 대응 결의서 채택 - 회원국의 보안제도 평가, 대응 권고	2001년 11월
WCO	총 회	○ 새로운 공급사슬 보안제도 도입 - CSI · C-TPAT 모델의 세계 규범화	2005년 7월 확정
민 간 부 문	허치슨, 싱가포르PSA	○ Smart and Secure Tradelane - 민간 차원의 해사보안 프로그램	2002년 7월

자료 : 한국해양수산개발원

이와 함께 미국 해운보안법은 외국항만에 대한 보안평가를 크게 다음과 같은 여섯 가지 기준에 따라 시행할 것을 규정하고 있다.

첫째, 컨테이너 화물과 기타 일반화물, 그리고 수화물에 대한 검색이 올바르게 이루어지고 있는지 여부,

둘째, 화물 · 선박 및 부두 지역 등 출입통제지역에 대한 보안조치가 적절하게 이루어지고 있는지 여부,

셋째, 선박에 대해 적절한 보안조치가 이루어졌는지 여부,

넷째, 적절한 보안기준의 이행을 확인할 수 있는 증서나 서류 등이 갖추어졌는지 여부,

다섯째, 외국 항만의 보안관리 프로그램의 효율성

여섯째, 미국에 대한 테러를 억지하는 데 필요한 적절한 조치가 시행되고 있는지 여부 등이다.

마지막으로 외국항만에서 시행하고 있는 보안조치의 유효성을 평가한 다음에 미국이 취할 수 있는 조치로 해운보안법은 크게 2가지 사항을 규정하고 있다. 즉, 외국항만에 대한 보안평가 결과 그 항만이 테러를 막는 데 필요한 조

치를 강구하고 있지 못한 것으로 판단된 경우에는 그 결과와 함께 적절한 개선대책을 마련하라고 해당 국가에 권고할 수 있다는 점이다. 이 경우 미국은 외국항만의 보안기능을 제고하기 위해 항만보안훈련 프로그램을 운영할 수 있다. 이 같은 조치는 결국 자국이 요구하는 보안수준에 미달하는 국가에 대해서는 미국이 직접 보안프로그램 가동을 지원한다는 의미로 해석된다.

이 같은 조치와 함께 미국은 외국항만이 효과적인 반테러조치를 시행하지 않는다는 결과가 나온 경우에 미국의 입항을 통제하는 3가지 조치를 내릴 수 있다. 일정한 조건을 붙인 입항허가, 일정한 조건을 붙이는 데 문제가 있는 때에는 입항 금지, 그리고 그 같은 사실에 대한 대외적인 공표 등이 그것이다. 다만 보안조치가 미비한 외국항만에서 입항하는 선박에 대한 통제는 해당 국가에 그 같은 사실을 통보한 이후 90일이 지나야 가능하다. 예외적으로 미국 해운보안법은 국토 안보부 장관에게 국무부 장관과 협의 결과 해당 항만의 보안상태가 여객이나 선원 등이 이용하고, 선박이 입항하는데 위험을 준다고 판단한 경우에는 ‘90일 경과 기간’과 관계없이 즉시 필요한 조치를 발동할 수 있도록 규정하고 있다.⁶⁴⁾ 그리고 외국항만이 미국에서 요구하는 일정한 보안요건을 충족한 때에는 해운보안법에서 규정하고 있는 입항 제한 조치 등이 해제된다.

6) 연안경비대 등의 운수 근로자 신분 통제

선박 및 항만보안업무를 전담하고 있는 연안경비대(USCG) 또한 9·11 테러 이후 미국 361개 항만과 연안해역에서 입항선박과 선원·항만근로자를 대상으로 보안 통제를 대폭 강화하고 있다. 연안경비대의 물류보안 강화 조치 가운데 가장 대표적인 것은 선원·여객 및 적하목록을 검사할 시간을 확보하기 위해 외국 선박에 대한 입항 예정시간 통보를 종전의 24시간 전에서 96시간 전으로 변경한 것이다.

64) 선박에 대한 입항 통제뿐 아니라 미국 해운보안법은 각 규정을 위반한 모든 사람에 대해 위반할 때마다 2만 5,000달러 이하의 벌금을 부과하도록 규정하고 있음.

이와 함께, 연안경비대는 테러리스트 선박에 의한 공격에 대비하기 위하여 주요 항만·해역에 124개소의 보안지역을 설정하고, 이 규정을 위반한 선박에 대해서는 선박 몰수, 6년 이하의 징역, 25만 달러의 벌금에 처하는 우범자에 대한 통제를 강화하고 있다. 특히 미 연안 경비대는 해상에 대한 순찰 강화뿐만 아니라 테러리스트가 수중을 침투할 수 있다는 판단에 따라 중요 시설에 대해서는 차단망을 설치하고, 수중 다이버 등을 활용, 수색활동을 정례화하고 있다.

또한 미국은 최근에 항만 근로자를 포함한 운수 근로자를 대상으로 한 대대적인 신분조사 작업에 착수하였다. 미국 국토 안보부는 2006년 4월 교통보안청과 연안경비대가 중심이 되어 40만 명에 달하는 항만 하역 인부와 기타 항만 근로자들을 대상으로 성명을 확인하고, 신분증을 다시 발급하는 제도를 시행할 방침이라고 밝혔다.

이 같은 조치는 최근 디피 월드의 미국 항만 터미널 인수 문제를 계기로 불거진 항만 보안을 강화하고, 불법 이민자들을 색출하기 위한 것으로 풀이되고 있다. 미첼 체토프 국토 안보부 장관은 기자 회견에서 교통보안청의 경우 곧바로 항만에 정기적으로 출입하는 근로자의 이름을 확인하는 작업에 착수하였다. 미 연안경비대는 자체적으로 개설한 홈 포트라는 웹을 통해 항만 근로자를 고용한 회사가 근로자 명단을 제출하면 이를 토대로 신원 확인 절차에 착수할 예정이다.

미 국토 안보부는 이 같은 작업이 앞으로 3년 동안 추진할 ‘교통 근로자 신분 확인 및 증명서 발급 제도⁶⁵⁾’를 완전히 이행하기 위한 기초 작업이라고 밝히고, 미 의회의 경우 현재 근로자 신분 확인제도를 조속히 시행할 것을 요청하고 있는 상태라고 덧붙였다. 미국은 근로자 이름 검색 작업은 미 해운보안법에 따라 시행하고 있는 항만 근로자에 대한 범죄 경력조회제도를 보완하는 기능이 있다고 강조하고, 이 업무를 보다 신속하게 처리하기 위해 해당 업체에 대해 근로자 신분을 조회할 수 있는 데이터베이스를 설치·운영할 것을 권고

65) the US Transportation Workers Identification Credential Programme.

하고 있다.⁶⁶⁾ 그러나 이 같은 조치를 도입하는 것과 관련하여 미국의 운수노동조합을 포함한 해운업계 및 트럭 운송업체 등에서는 일제히 우려하는 목소리를 내고 있다.

첫째, 미국 항만 당국은 자체적으로 이 제도를 시행하는 데 앞으로 10년 동안 2억 9,000만 달러에서 3억 2,500만 달러가 소요될 것으로 추정하고 있다. 또한 항만 근로자의 경우 신분증을 발급받는 데 1인당 109달러의 발급 수수료를 내야 하는 부담이 있다고 비판하고 있다. 미국 전체적으로는 10억 달러 이상의 비용이 들어간다는 것이 일반적인 시각이다.

둘째, 신원 조사 과정에서 상당수의 운수 근로자들이 신분증 발급을 거절당할 가능성이 크다는 점이다. 미국 국토 안보부는 앞으로 3년 동안에 항만 근로자와 트럭 기사, 터미널 종사자들을 대상으로 이민 기록과 범죄 기록 및 테러조직과의 연계 등 가능한 한 모든 수단을 동원하여 신원조사를 진행할 예정인데, 이 과정에서 적지 않은 부적격자가 나타날 가능성이 크다고 분석하고 있다.⁶⁷⁾ 특히 컨테이너 트럭 운송업체의 경우 멕시코 계 무자격 기사가 많아 향후 결과 여하에 따라 인력 부족 현상이 심화될 가능성도 배제할 수 없다고 강조하고 있다.⁶⁸⁾

7) 항만보안법 제정 · 시행

미국의 조지 W 부시 대통령은 2006년 10월 13일, 중간 선거를 앞두고 그동안 많은 논란을 불러일으켰던 항만보안법(SAFE Port Act)을 공포했다. 이에 따라 미국은 2002년에 제정된 해운보안법과 함께 해운 및 항만 분야에 걸쳐

66) *Journal of Commerce*, 2006. 4. 25.

67) *Fairplay*, 2006. 6. 8.

68) 한편, 캐나다 또한 미국과 유사한 항만 근로자 신원조사제도를 조만간 도입할 계획임. 캐나다 연방 교통부는 관련 법률을 개정해 2단계로 항만 근로자에 대한 신원조사에 착수하되, 밴쿠버 항만과 할리팩스와 몬트리얼 항만, 세인트 로렌스 해로에 대해 1단계 조사를 실시하고, 브리티시 컬럼비아 항만, 프린스 루퍼트 항만, 프레이지 강은 2단계 사업에 포함시켰음. 캐나다는 이번 조사에서 항만 근로자뿐만 아니라 도선사, 항만 보안 담당관, 그리고 자격을 갖춘 선원에 대해서도 신원조사를 실시할 방침임(*JOC*, 2006. 6. 29).

거의 완벽한 보안 시스템을 갖추게 됐다. 전문가들은 항만보안법이 명칭과 달리 물류 전반을 적용대상으로 하고 있어 향후 파급효과가 클 것으로 보고 있다.

그 동안 미국에서는 항만보안법 제정과 관련해 적지 않은 논란이 제기돼 왔다. 국토안보부가 현재 시행하고 있는 제도만으로는 대량살상무기(WMD)를 효과적으로 차단하는데 한계가 있고, 지난 3월의 디피 월드 파동을 계기로 미국의 항만보안을 강화해야 한다는 의견이 강력하게 대두됐기 때문이다. 특히 미국 수입 컨테이너 화물에 대한 100% 사전 검색이 주요쟁점으로 떠올랐다.

항만보안법은 이 같은 미국의 우려와 걱정을 적절하게 수렴한 종합 물류보안법이다. 법률 전반에 컨테이너 화물을 운송하는 과정에서 일어날 수 있는 테러 방지에 초점을 맞추고, 다양한 조치를 마련해 놓고 있기 때문이다. 기존에 시행하고 있던 컨테이너 보안협정(CSI) 등을 입법화하고, 100% 화물검색을 위해 외국항만을 선정해 ‘시범사업’을 하도록 한 것이 특히 그러하다.

이와 함께 항만보안법은 기술적인 한계 때문에 결정을 미뤘던 컨테이너 보안 표준과 화물검색기 문제에 대해서도 입장을 정리했다. 2006년 말까지 컨테이너 보안 표준안을 발표하고, 차세대 검색기 개발에 박차를 가하도록 방침을 정했다. 물류보안을 강화하는 데 필요한 국가계획을 수립하고, 테러가 발생한 경우 신속한 복구와 교역 재개 방안을 마련하도록 한 것도 큰 수확으로 평가되고 있다.

〈표 4-5〉 SAFE Port Act 중 국제물류 관련 주요내용

SEC. 201.(f)	○ 국토안보부 장관은 외국정부와 국제기구의 기준과 시행조치를 고려하여 국제물류공급망에서의 컨테이너 화물의 보안을 위한 기준을 정하여야 함
SEC. 202	○ 국토안보부 장관은 보안사고시 무역의 재개를 위한 계획을 개발해야 함 - 이 경우 다음과 같은 선박에 우선권을 줄 수 있음 · 유효한 International Ship Security Certificate를 보유한 선박 · C-TPAT 참가자에 의해 운영되는 선박 등 - 화물의 경우 · CSI가 시행되는 항만에서 직접 운송된 화물 · C-TPAT 참가자에 의해 운송된 화물 · 방사성 검사, X-RAY, imaging scan 또는 입항전 항만에서 컨테이너를 검증할 수 있는 시스템(동 정보가 미 세관국경보호국에서 평가, 분석 된 경우) 등을 거친 화물

〈표 4-5〉 SAFE Port Act 중 국제물류 관련 주요내용(계속)

SEC. 203	○ 국토안보부 장관은 고 위험도 화물을 식별하기 위해 자동 타겟 시스템을 구축해야 함
SEC. 204.(C)	○ 국토안보부 장관은 외국정부, 국제기구 등과 국제물류공급망에서의 컨테이너 화물보안을 위해 국제적인 기준을 정할 수 있음
SEC. 205	○ 국토안보부 장관은 외국항에서 미국내로 반입되는 해상 컨테이너를 점검하기 위해 CSI 프로그램을 시행해야 함
SEC. 211	○ 국토안보부 장관은 국제 물류공급망에서의 보안 강화를 위해 C-TPAT를 시행할 권한을 가짐. 또한 최소 1년에 한번씩 C-TPAT의 보안 요구사항을 검토하고 필요한 경우 최신화 하여야 함
SEC. 212	○ 수입업자, 세관브로커, 포워더, 항공, 해상 및 육상 운송업자 등 국제물류공급망에 속한 자는 자발적으로 C-TPAT에 참가할 수 있음
SEC. 213	○ C-TPAT에 참가를 원하는 자는 국토안보부에서 정한 보안 기준을 토대로 물류공급망에 대한 평가를 시행하여야 함 - 보안기준 : business partner requirements, container security, physical security and access control, personnel security, procedural security, security training and threat awareness, information technology security 등
SEC. 214~216	○ C-TPAT는 참가정도에 따라 3단계로 나누어지며 각 단계별로 타겟 시스템 평가점수의 축소, 화물검색의 저감과 화물 우선검사 등의 혜택을 부여함
SEC. 231	○ 법령 발효 후 90일 이내에 국토안전부 장관은 ‘nonintrusive imaging equipment’와 ‘radiation detection equipment’를 결합한 ‘integrated scanning system’을 시행할 해의 3개항만을 정하여야 함 - 아울러, 미국행 컨테이너에 대한 완전한 검색과 이에 대한 이미지 및 각종 정보가 미국내 평가, 분석을 위해 제공 되도록 하는 등 법령 발효 후 1년 이내에 동 시스템의 시행을 위한 조치가 이루어져야 함
SEC. 232	○ 국토안보부 장관은 산업에너지부, 외국파트너와의 협력을 통해 가능한 빠른 시간내에 미국으로 유입되는 모든 컨테이너에 대해 도착전 ‘integrated scanning system’을 통해 검사되도록 하여야 함
SEC. 233	○ 국토안전부 장관은 국무성, 산업에너지부 등과 CSI를 시행하고 있는 항만에서의 물류 공급망 보안 조치를 촉진하기 위해 기술, 장비 및 훈련에 관한 사항을 지원할 수 있음
SEC. 235	○ 국토안전부 장관은 미국내 항만에서 공 컨테이너에 대한 보안을 강화하기 위한 파일럿 프로그램을 시행하여야 함

자료 : 미국 항만보안법 자료를 이용, 해양수산부 작성

8) 시사점

미국은 2001년 9·11 항공기 테러의 최대 피해국으로, 현재 국제적으로 시행되고 있는 물류보안제도의 표준을 제시하고 있다. 이에 따라 미국이 제정하거나 도입하고 있는 각종 물류보안 강화조치는 거의 빠짐없이 국제기구에서 국제 협약이나 결의 형태로 도입되고 있다. 미국의 물류보안제도에 관심을 기울여야 하는 이유가 바로 여기에 있다. 그런데 문제는 이 같은 경향이 앞으로 더욱 심화될 가능성이 크다는 점이다. 미국 의회는 2006년 10월 13일 항만보안법을 제정하면서 앞으로 국제사회에 영향을 미칠 수 있는 여러 가지 규정을 포함하였다. 컨테이너 화물에 대한 100% 검색 시범 사업, 컨테이너 보안장치에 대한 국제 표준화 작업 촉진 등이 대표적이다. 미국의 물류보안제도에서 얻을 수 있는 시사점을 정리하면 다음과 같다.

첫째, 물류보안제도가 앞으로도 한동안 지속되고, 강화될 것이라는 점이다. 미국은 2002년에 해운보안법을 제정한 이후 여러 가지 물류보안을 강화하는 조치를 취해 왔다. 그러나 2006년 2월 디피 월드의 미국 내 피앤 오 포츠(P&O Ports)의 6개 터미널 인수 문제가 불거진 이후 항만보안법을 다시 제정하였다. 이 같은 항만보안법 자체가 앞으로 미국의 교역 상대국에 상당한 영향을 담고 있을 뿐만 아니라 미국은 내륙 물류보안을 강화하는 입법 조치도 아울러 검토하고 있기 때문이다. 미국의 물류보안동향은 우리나라 수출 기업에 즉각적인 영향을 미치므로 신속하게 대처하는 노력이 필요하다. 필요하다면, 민관 물류보안 정보 협력 체제를 구축하는 것도 바람직하다.

둘째, 미국 수출 기업뿐만 아니라 해외에 상품을 판매하는 기업들은 앞으로 더욱 엄격해질 컨테이너 화물 검색제도에 대비해야 한다. 미국은 항만보안법에 시범사업에 대한 규정과 함께 향후 시행 가능성에 대한 검토를 수행하도록 규정하고 있다. 이뿐만 아니라 미국의 CSI와 C-TPAT를 모델로 한 세계세관기구(WCO)의 이른바 ‘프레임워크’도 조만간 국제적으로 시행될 것으로 보인다. 이렇게 되면, 미국에 컨테이너 화물을 수출하는 기업은 물론 다른 나라에 화물

을 수출하는 제조업체도 같은 영향을 받게 된다는 점에 유의할 필요가 있다.

셋째, 물류보안 산업이 새로운 비즈니스 모델로 떠오르고 있는 점에 대해서도 관심을 기울여야 한다. 아직 시장이 형성되는 초기이기 때문에 구체적으로 그 개념과 시장 규모가 파악되지 않고 있다. 다만, 미국의 록히드 마틴이나 GE 등 글로벌 기업들은 물류보안 시장을 선점하기 위해 적극 나서고 있는 것은 분명하다. 앞으로 컨테이너 화물 검색기와 컨테이너 보안 장치(CSDs), 컨테이너 화물 추적 시스템, 제조업 및 항만보안의 시설 보안 시스템 구축, 물류보안 컨설팅 등이 유망업종으로 등장할 가능성이 크다.

2. EU의 물류보안제도

1) 현행 EU 물류보안 여건

유럽연합(EU)의 물류보안제도는 국제적으로 시행되고 있는 보안제도를 근간으로 하고 있다. 그러나 최근 유럽연합은 국제 선박 및 항만시설 보안에 관한 규칙(ISPS Code)에서 임의규정(Part B)으로 되어 있는 사항도 강제화하는 등 보안조치를 강화하고 있다. 또한 유럽연합은 기존의 ISPS Code로는 물류 전반에 대한 보안확보가 현실적으로 불가능하다는 판단에 따라 2006년 2월에 ‘물류보안 기본규칙’을 수립하여 시행한다는 방침을 천명하였다.

유럽연합은 이 지침에서 기존의 ISPS Code에서 포함되지 않은 철도 및 도로 등 내륙 교통부문의 보안조치를 강화하는 한편, EU의 인증을 받은 운전자(Secure Operator Scheme)에 대해서는 최소한의 검사를 보장하는 등 보안 검사제도를 줄이는 제도를 도입할 방침이다.

그러나 유럽연합의 이러한 방침에 대해 화주 등 이해관계자들이 강력하게 반발함에 따라 올해까지 입법조치가 불가능하다는 의견이 제시되고 있기 때문

이다. 화주들은 이 제도를 도입에 따른 구체적인 실익이 없고, 행정적인 절차가 복잡할 뿐만 아니라 인증사업자의 범위도 매우 애매하다고 보고 있기 때문이다. 그러나 유럽연합은 이 같은 우려에도 불구하고, 2006년 12월에 물류보안기본규칙을 정식으로 채택하였다.

이 규칙은 2005년 10월에 채택된 세계관세기구(WCO) 협정을 기반으로 화물에 대한 보안 강화, 물류보안 인증 사업자에 대한 통관처리 간소화, 세관 당국 간의 화물 정보의 전자적 교환 등을 핵심으로 하고 있다. 특히 유럽연합은 이 규칙을 통해 i) 회원국에 대해 즉시 화물 및 사업장에 대한 위험 관리체제를 구축하고, ii) 물류보안인증 증서를 발급(2008년 1월부터)하는 한편, iii) 수출입 화물 정보의 사전 제출을 의무화(2009년 7월 1일)하고, iv) 컨테이너 화물의 수출통관 과정에서의 세관 당국 사이의 화물정보 교환을 촉진(2007년 6월 30일까지)한다는 방침이다. 유럽연합의 물류보안제도를 집중 분석하였다.

(1) EU의 물류보안 규정

① 민간항공 법률

2002년에 제정된 유럽연합 민간항공 보안규정(Regulation EC n° 2320/2002)은 민간항공에 대한 불법적인 방해 행위를 막기 위하여 유럽연합이 제정한 특별법이다. 이 법률은 보안에 관한 공통의 기초적인 기준을 설정하고 있다. 즉, 일반적으로 수용 가능한 감시 메커니즘을 만들고, 시카고 협약(Chicago Convention) 관련 조항들의 보편적 해석을 위한 기준을 제시하고 있다.

한편 2006년 11월 6일부터 영국, 프랑스, 독일, 이태리 등 25개 EU회원국과 스위스, 노르웨이 및 아이슬란드의 공항에서 세계각지로 출발하는 항공기 탑승객에 대해 신항공보안 규정이 적용되고 있다. 이는 지난 8월 10일 영국에서 영국-미국 노선의 항공기 10대를 액체폭약으로 폭파시키려던 시도가 실패로 돌아간 사건 이후 대책으로 나온 것으로 100ml를 넘는 용기에 담기는 모든 액체, 젤류, 페이스트류, 에어줄은 기내로 소지하고 탑승할 수 없다. 이에 따라

여행객은 두 가지 방법을 사용할 수 있다. 이를 화물로 실어 보내든지, 이 물품이 여행 중 꼭 필요하다면, 20cm × 20cm 크기의 지퍼가 달린 비닐봉투에 병이나 튜브를 담아야한다. 하지만 이 역시 100ml를 넘길 수 없다. 이 규정에도 불구하고 다음의 두 가지 물품은 예외이다. 비행기에 탑승한 아이를 위한 분유(이는 젖병이 100ml가 넘어도 상관없다). 이 경우 보안검색시 아이와 함께 탑승하는 보호자에게 이를 먹어보라고 요구할 수 있다. 또 다른 하나는 인슐린이나 시럽 등의 의약품인데, 이 역시 의사의 처방전이나 질병 증명서 등의 서류를 제출하여야 한다.

② 해상 및 항만시설보안 규정

유럽연합은 해상 및 항만분야와 관련하여 국제적으로 인정된 조치들을 지지하고 있으며, 유럽의 항만과 유럽 항만에 기항하는 선박들에 대하여 국제적으로 요구하는 조치를 이행하고 있다. 유럽연합의 해운 및 항만시설 보안규정(Regulation EC n° 725/2004)은 IMO의 해상인명안전에 관한 국제협약(SOLAS)과 ISPS Code의 내용을 수용하고 있다. 특히 ISPS Code는 강제조항인 Part A와 권고사항인 Part B로 구성되어 있는 반면에 이 규정은 회원국의 국제여객 운송분야에서 ISPS Code의 권고사항인인 Part B의 특정조항도 강제로 적용하고 있다. 즉, 국제항해에 종사하는 A 등급 여객선에 대하여 2005년 7월 1일 이후부터 IMO에서 요구하는 보안조치를 강제화하고 있다. 이는 유럽연합의 해상보안 수준을 강화시키면서 왜곡된 경쟁을 유발하거나 국민과 재화와 관련된 취약한 분야의 보호 등 일부 이해관계에 있는 분야에 관한 회원국 간의 해석의 차이를 피하기 위한 조치이다.

③ 항만보안 강화 지침

유럽연합은 2005년 10월에 항만보안을 강화하는 지침서(Directive 2005/65/EC)를 채택하였다. 이에 따라 회원국들은 2007년 6월까지 이 지침에 따른 조치를 취하여야 한다. 이 지침은 ISPS Code의 적용대상이 선박과 육상의 직접적인

점점에 한정되는 것을 보완하기 위한 것이다. 즉, 항만은 보안에 민감한 부분들과 그렇지 못한 부분으로 구성된 복잡한 지역인 점을 고려하여 각 항만에 적합한 절차를 만드는 것을 허용하기 위한 것이다.

보안 평가는 보안조치를 위한 필요조건이며, 항만보안조직 및 관련당사자들과 의사소통 채널의 효율성도 항만보안 평가의 한 부분이 된다. 이러한 결과로 각 항만의 보안계획은 지정된 항만보안당국에 의해 수립되고 보증되는 한편, 상기에 언급한 해상보안규정의 규율을 받는 화물을 수출하거나 취급하는 모든 항만에 적용된다.

(2) EU 공급망 보안의 문제점

항공분야와 해상 및 항만분야의 보안조치들이 만족스럽게 이행되고, 인적 실수가 제거된다고 하더라도 이는 전체 물류운송체계, 즉 공급망 중 특정분야의 보안이 확보되는 것에 불과하다. 따라서 전체 공급망의 보안확보 문제는 여전히 남아 있다. 공급망의 보안확보가 어려운 점은 다음과 같다.

첫째, 공급망은 제조업자에서 시작하고 화물의 종착지에서 끝난다. 만일 보안이 불완전한 물품(예: 오염된 물품)을 선적한 선박이 출항한 이후에는 후속적인 보안조치로 보안사고를 방지하는 것은 극단적으로 어려운 일이다. 이에 따라 물품이 선박에 선적되기 이전에 만족스러운 보안수준을 확보되어야 한다.

둘째, 매일 수백만의 공급망이 가동되고, 공급망의 다양한 수송활동에 참여하는 업자가 적어도 50만 이상이다. 이들은 운송, 포워딩, 보관, 하역, 창고업, 육상 터미널 운영 등에 참여하고 있으며, 그기에 화주, 중개자, 도매업자가 추가되고 있는 실정이므로, 실질적인 보안을 확보하는 데 난점이 있다.

셋째, 최근의 추세는 컨테이너 일괄운송에 초점이 맞추어져 있지만 컨테이너가 유일한 잠재적인 목표가 아니라는 점이다. 유럽연합 역내무역은 컨테이너만큼 다른 교통수단(스윙바디)에 의존하고 있는데 이러한 교통수단도 테러리스트의 공격을 당할 위험이 컨테이너만큼 크다. 실제적인 관심은 위험이 전가되는 모든 화물수송형태에 대해 어떠한 방식으로든 보안기준을 적용해야 하는

점이다.

넷째, 정기적으로 항공 또는 해운을 이용하지 않는 공급망 운영자는 낮은 보안 의식을 가지고 있다. 이에 따라 모든 운영자에 대한 높은 수준의 보안규정을 적용하는 것은 일괄 공급망의 붕괴를 초래할 우려도 있다.

2) EU 물류보안 여건개선 노력

(1) 유럽연합 이사회 의결

유럽연합 이사회(European Council)⁶⁹⁾는 2004년 3월에 테러행위에 대응하기 위한 특별법안 제정이 필요한 분야로 수송과 에너지 분야를 규정하면서, 법률체제의 강화와 예방 메커니즘의 향상을 포함한 모든 형태의 운송시스템의 강화를 의결하였다. 또한 집행위원회(EC)에게 유럽이사회와 회원국의 승인을 받아 테러행위에 대처하기 위한 메커니즘(감시, 조기경보, 정보발생 및 응답체계와 절차)의 구축뿐만 아니라 시민과 필수서비스(상수도, 에너지, 통신), 생산 시스템(농식품, 장치산업)의 보호를 강화하기 위한 정책 개발을 요구하였다.

(2) 유럽연합 집행위원회 조치

① 유럽연합의 공급망 보안강화 목표설정

유럽연합 집행위원회는 유럽연합 이사회의 지시에 따라 유럽연합의 전 운송 구간의 물류보안을 강화하는 방안을 검토하였다. 우선 예상되는 테러리스트의 공격으로부터 전 유럽의 화물운송의 보호를 향상시키는 것을 목적으로 삼고, 그 목적 달성을 위한 목표를 다음과 같이 설정하였다.

첫째, 자유무역의 흐름을 방해하지 않고, 공급망에 따른 보안을 강화한다는 것이다. 높은 수준의 보안을 요구할 경우 자유무역 흐름의 강화 요구와 충돌이

69) 유럽연합 이사회(European Council)는 EU 국가의 정상들로 구성되어 있음.

발생하므로 양자간의 균형관계 유지가 필요하기 때문이다.

둘째, 통상 운송시장과 현존 보안조치를 위협하지 않고, 유럽연합이 체계적으로 접근하기 위한 기본골격을 만드는 것이다. 항공 및 해상운송은 세부적인 보안규칙이 있고, 그에 따라 적절한 조치를 취할 수 있는 강력한 보안수준을 유지하고 있다. 이러한 것은 항공 및 해상운송 시장이 지리적으로 한정되거나 제한된 통제가 가능한 영역에서, 제한된 숫자의 운영자에 의해 운영되기 때문에 가능하다.

그러나 육상운송의 공급망은 이와는 상당히 다른 구조를 가지고 있다. 즉, 육상운송에는 아주 다양한 문화와 영업형태를 가진 다국적 기업에서부터 영세 서비스회사에 이르기까지 약 50만개 이상의 회사가 운송 및 부대서비스에 관련되어 있다. 그리고 이들 회사는 대부분 보안관리를 하지 않거나 시작하는 단계에 있으므로 육상운송 공급망에 대해 해상이나 항공운송과 같이 단일의 포괄적인 보안운영체계를 설립하는 것이 불가능하다. 그러므로 기술진전과 운영 환경에서 만족한 보안수준을 보장하기 위하여 위험개발의 정도에 따라 점차적으로 발전할 수 있는 최저보안요건에 관한 체계 설립이 보다 현실적이다.

셋째, 유럽연합 차원 및 각국 차원에서 불필요한 행정적 절차나 부담을 피해야 한다.

② 집행위원회의 제안

유럽연합 집행위원회는 예상되는 테러리스트의 공격으로부터 유럽연합의 공급망 보안을 강화하기 위하여 다음과 같은 조치를 제안하였다.

첫째, 회원국들은 유럽의 최소한의 보안수준을 만족시키는 공급망 운영자에게 부여하고, 내부 시장에서 상호 승인되는 보안품질 라벨(인증받은 운영자)을 만들기 위한 강제적인 시스템을 도입한다.

둘째, 회원국에 대한 강제적 조항내에서 공급망 운영자가 인센티브를 받는 대신에 그들의 보안이행을 향상시키기 위한 자발적 계획을 도입하게 한다.

셋째, 유럽 화물 운송에서 보안이행에 대한 공급망 운영자 책임제도를 도입한다.

넷째, 보안활동을 수행하고 보안 분야에서 다른 경쟁자들보다 긍정적 위치로 분류되기 원하는 ‘보안인증을 받은 운영자(secure operator)’에게 상업적 경쟁우위를 갖게 하는 혜택을 부여하는 것을 허용한다.

다섯째, 승인된 국제기준을 포함한 보안의 필요조건을 정기적으로 향상시키고 개량하는 것을 허용한다.

여섯째, 유럽연합 감시제도를 통하여 회원국의 이행을 감시한다.

여기서 중요한 개념이 민간을 공급망 보안시스템에 자발적으로 참여시키기 위한 보안 인증 운영자 제도(secure operator scheme)의 도입이다. 이 제도는 요구되는 최저수준의 보안 요건을 갖춘 운영자에게 특정의 지위를 부여하고, 그러한 지위를 받은 자에게 여러 가지 혜택을 주는 것을 주요 골자로 한다. 공급망 운영자가 책임당국으로부터 특별한 지위를 부여받기 위해서는 보안강화를 위한 계획을 자발적으로 수립·이행하여야 한다. 공급망의 운영자가 자발적 계획 수립을 통해 공급망 보안에 참여하는 것은 보안 책임당국과 운영자 모두에게 실질적인 이득이 된다. 이들에게 주어지는 혜택은 다음과 같다.

첫째, 공공자원을 효율적으로 이용할 수 있다. 보안 책임당국은 계획에 참여하지 않는 운영자에게 그들의 통제자원을 집중할 수 있다. 그러면서 인증된 운영자는 자발적으로 계획에 의해 공급망 보안에 참여하기 때문에 이들에 대한 통제권도 상실되지 않는다. 동일한 방법은 관세당국이 공인 경제운영자(Authorized Economic Operator)에 적용하여 성공한 것으로 판명되었다. 보안 책임당국은 통제자원을 집중해서 업무를 수행할 수 있어 공공자원의 효율적 이용에 의해 혜택을 얻게 된다.

둘째, 안전한 해상 및 항공 수송의 상호연계성을 확보할 수 있다. 엄격한 유럽연합 보안규정에 있는 항만시설을 포함한 항만과 공항에서는 승인된 운영자(SC)를 통해 들어온 화물은 적절하게 보안이 되었다는 것을 확신할 수 있다.

따라서 그러한 운영자에게는 예컨대 그린 레인(green lane) 사용권 부여 등 우선권을 준다.

셋째, 범 유럽연합의 승인이 가능하다. 한 국가 당국에서 부여한 승인받은 운영자의 지위에 대한 범 유럽연합의 승인은 운영자와 회원국에 모두에게 이익이 된다. 운영자는 EU를 통한 승인으로 혜택을 볼 것이고, 그러한 지위부여가 통일된 유럽연합의 절차에 따른 것임을 알고 있는 회원국은 타 회원국에 의해 합의된 유럽연합의 최소한의 요건을 적용한 지위부여를 신뢰할 수 있을 것이다.

넷째, 글로벌 공급망 보안의 통합을 촉진한다. 수출입 양측에 대하여 국경 외부의 보안을 통제하는 관세당국은 공인 경제운영자(AEO)제도 속에서 승인된 운영자의 보안지위를 인정할 수 있어 이러한 지위가 부여된 운영자는 신속한 통관을 기대할 수 있다.

다섯째, 보안의 유지에 따른 사업상 효과도 증대된다. 승인된 운영자는 자신이 운송하는 화물이 공급망 상의 보안간섭으로부터 면제받을 수 있어 의뢰인과 공급망 파트너로부터 신뢰를 얻을 수 있다.

여섯째, 다른 보안부문과 연계하는 경우 시너지 효과를 올릴 수 있다. 다른 부문의 사업자가 이 제도에 참여함으로써 혜택을 얻을 수 있다. 해상운송 부문에서 도입된 컨테이너 보안협정(CSI)가 제도 이외에 부수적인 효과를 가져온 것과 같은 이치이다. 즉, 운영시스템의 효율적인 통제와 운송 및 여타 과정에서 예측성 제고, 그리고 물류 부문의 가시성을 확보할 수 있어 예기치 않은 손실을 감소할 수 있는 것이 그것이다.

3) EU 공급망 보안강화 규정

유럽연합 집행위원회는 공급망 보안을 강화하기 위하여 2006년 2월에 공급망 보안강화 규정(안)을 채택하여 유럽연합 의회 및 유럽경제사회이사회 및 지역위원회에 이송하였다. 이 규정(안)은 유럽연합 의회와 유럽연합 이사회가 채

택하기 전까지 활발한 토론을 거치고 있다. 이하에서 이 규정의 주요내용을 살펴본다.

(1) 규정의 목적

이 규정은 보안사고의 위험에 직면한 육상운송 공급망⁷⁰⁾의 보안을 강화하기 위한 것이다. 유럽연합은 i) 회원국이 승인된 운영자(secure operator)의 지위 부여에 대한 계획 수립, ii) 승인된 운영자(secure operator) 지위부여를 위한 최소한의 필요요건 준비 및 iii) 적정한 감시 메커니즘 구축을 통해 이러한 목적을 달성할 계획이다(제1조).

(2) 적용 범위

이 규정은 공급망 보안, 화물 및 운송보안, 그리고 유럽연합 영토내의 공급망과 관련 있는 기반시설에 적용한다. 특히 이 규정에서 정하고 있는 조치는 다음의 활동과 관련있는 운영자에 대해 적용한다. i) 화물의 선적 준비와 생산지에서 화물의 선적, ii) 화물의 운송, iii) 화물의 주선, iv) 창고, 보관 또는 내륙터미널 운영,

그러나 이 규정을 다음의 규정의 적용을 배제하지 않는 점에 유의할 필요가 있다. i) 민간 항공 보안 분야에 관한 유럽연합 규정, ii) 선박 및 항만 시설 보안 강화에 관한 유럽연합 규정, iii) 항만보안에 관한 유럽연합 규정, iv) 위험화물 및 핵물질 수송에 관한 유럽연합 및 국제 규정, v) 유럽연합 관세 규정 등이 이에 해당된다.

(3) 책임기관

회원국은 이 규정에서 정한 공급망 보안조치의 적용을 조정, 이행, 감시하는데 필요한 공급망 보안의 책임기관을 지정하여야 한다.

70) 공급망의 정의 : 운송에 관한 준비와 유럽연합 영토 내의 생산지에서 배송지점까지의 화물의 육상 운송을 포함하는 모든 과정과 운영자를 의미한다(제2조).

(4) 승인된 운영자

① 지위부여에 대한 계획수립

회원국은 유럽연합 공급망 보안 강화 규정이 채택될 경우, 18개월 이내에 승인된 운영자 지위 부여에 관한 계획을 수립하고, 그 사실을 유럽연합 집행위원회에 통지하여야 한다(제7조).

② 승인된 운영자가 될 수 있는 자

승인된 운영자가 될 수 있는 자는 다음에 열거하는 업무에 종사하는 자이어야 한다. i) 화물의 선적 준비와 생산지에서 화물의 선적, ii) 화물의 운송, iii) 화물의 주선, iv) 창고, 보관 또는 내륙터미널 운영 등이다.

③ 승인된 운영자의 혜택

회원국 중 한 국가에서 ‘승인된 운영자’ 지위를 부여받은 경우는 모든 회원국에서 그 지위가 인정된다. 승인된 운영자는 회원국의 보안통제조치를 편리하고 간편하게 받을 수 있다(fast track treatment : 우선 처리 혜택). 편리하고 간편하게 보안통제조치를 받는다는 것은 승인되지 아니한 운영자와 별도의 화물 통과나 절차를 받을 수 있는 것도 포함되어 있다. 한편 회원국은 다른 회원국의 승인된 운영자가 보안 규정에 심각한 위반을 하였을 경우에는 이 같은 혜택을 거부할 수 있다. 이 경우에는 그 사실을 다른 회원국과 위원회에 즉시 전달하여야 한다(제6조).

④ 승인된 운영자의 지위 부여 요건

승인된 운영자의 지위를 얻기 위해서는 보안 위반의 면책하에서 공급망의 일부분을 유지할 수 있는 운영자의 능력을 입증하여야 한다. 구체적으로는 보안 관리 시스템을 수립·시행·문서화하고, 지속적으로 개선시켜야 하는 것은 물론, 발생 가능한 보안위험에 대처할 수 있는 자원이 공급망의 일부임을 보증하

여야 한다. 그리고 화주, 운송회사, 운송주선회사 및 창고·보관 시설·육상터미널 운영자는 위험평가에 근거하여 보안관리시스템을 구축하여야 하며, 각각에게 요구하는 특정요건도 만족시켜야 한다(<표 4-6, 7, 8, 9> 참조). 이를 도표화하면 <그림 4-3>과 같다.

〈표 4-6〉 화주(생산지에서 화물의 선적준비와 선적관련 활동자)의 특별요건

항목	특별요건
물리적 보안	- 모든 건물과 재산이 불법진입·침입으로부터 보호될 것 - 다음 사항을 포함 • 내외부 문, 창문, 담장 등의 잠금장치 • 내부 및 주차장을 포함한 외부 시설의 조명 • 개인차량의 주차지역을 양적하 및 화물지역과 분리 • 내외부 통신시스템을 내부 보안인력 또는 지역 경찰들과 연결
접근 통제	- 양적하 및 화물지역의 불법접근 금지 - 통제는 다음 사항을 포함 • 고용자, 방문자, 사업관계자의 식별에 실패하지 않는 시스템 • 비승인, 미확인 인물에 대한 응대 절차
절차 보안	- 물품의 반입·반출 취급에 관한 조치는 물품구매, 교환, 분실과 관련한 보호 포함 - 보안절차는 다음을 포함 • 지정된 보안 담당자가 화물의 도입/이동을 감독 • 화물의 고유표식, 중량, 수량 파악 및 문서 작성 • 반입화물의 봉인 무결성 또는 다른 보안장치의 통제 • 반출화물의 봉인 및 다른 보안장치 시행 절차 • 부족 및 잔고의 검사 및 보고 • 반입, 반출 화물의 이동 추적 • 불법적 접근을 막기 위한 공재 또는 만재 용기의 적절한 보관 • 회사가 감지하거나 의심하는 변칙 또는 불법행위 설명 절차
인적보안	- 회사는 고용평등 및 개인정보보호에 관한 법률을 충분히 고려해서 장래 고용인에 대한 점검, 신청서 검증을 위한 내부 절차를 마련해야 함 - 내부 절차는 고용인의 이력 확인 및 특정 고용인의 관련 기능의 신뢰성에 대한 조사를 포함
문서화 절차	- 회사는 서류의 완결성, 판독성, 정확성 및 제출 시간을 확인
정보보안	- 공급망 상에서 정보전달 절차는 유지
교육 및 훈련 인식	- 예상되는 보안 위험 인식, 제품 무결성 유지 및 비권한자의 접근 한계 등이 포함된 보안 인식 프로그램을 고용자에게 제공

〈표 4-7〉 운송회사의 특별요건

항목	특별요건
물리적 보안	- 모든 건물과 재산이 불법진입·침입으로부터 보호될 것 - 다음 사항을 포함 • 내외부 문, 창문, 담장 등의 잠금장치 • 내부 및 주차장을 포함한 외부 시설의 조명 • 개인차량의 주차지역을 양적하 및 화물지역과 분리 • 내외부 통신시스템을 내부 보안인력 또는 지역 공간들과 연결
접근 통제	- 시설 및 운송수단에 대한 불법 접근 금지 - 통제는 다음 사항을 포함 • 고용자, 방문자, 사업관계자의 식별에 실패하지 않는 시스템 • 비승인, 미확인 인물에 대한 응대 절차
절차 보안	- 기록되지 않은 물질이 운송수단 또는 화물에 도입 되는 것을 막고, 불법적 인물의 접근을 막기에 적합할 것 - 보안절차는 다음을 포함 • 화물 및 화물장비의 고유표식, 수량 파악 및 기록(문서 작성) • 화물이 반입될 때 화물의 봉인 무결성 또는 다른 보안장치의 통제 • 화물 이양시 봉인 및 다른 보안장치 확인 절차 • 감시시스템 및 부족 보고 • 반입, 반출 화물의 이동 및 운송수단의 추적 • 불법적 접근을 막기 위한 공제 또는 만재 용기의 적절한 보관 • 회사가 감지하거나 의심하는 변칙 또는 불법행위 설명 절차 - 기록되지 않은 물질 또는 변경된 흔적 발견 시에는 운송수단의 접근 가능 부분과 운송수단 주변의 접근 가능 지역에 대한 물리적 검사가 수행 - 사건에 대한 보고 절차가 적합
인적보안	- 회사는 고용평등 및 개인정보보호에 관한 법률을 충분히 고려해서 장래 고용인에 대한 점검, 신청서 검증을 위한 내부 절차를 마련해야 함 - 내부 절차는 고용인의 이력 확인 및 특정 고용인의 관련 기능의 신뢰성에 대한 조사를 포함
문서화 절차	회사는 서류의 완결성, 판독성, 정확성 및 제출 시간을 확인
정보보안	공급망 상에서 정보전달 절차는 확실해야
승인된 화물흐름 조항 (Secure freight flow provisions)	- 회사는 승인된 운영자가 아닌 운영자가 제공한 화물을 확실할 수 있도록 검사하여 승인된 운영자의 화물 수준으로 향상시켜야 함 - 만약 검사가 시행되지 않거나 화물이 승인된 공급망의 “신속 조치” 부문의 화물로 판단되지 않는다면 거절

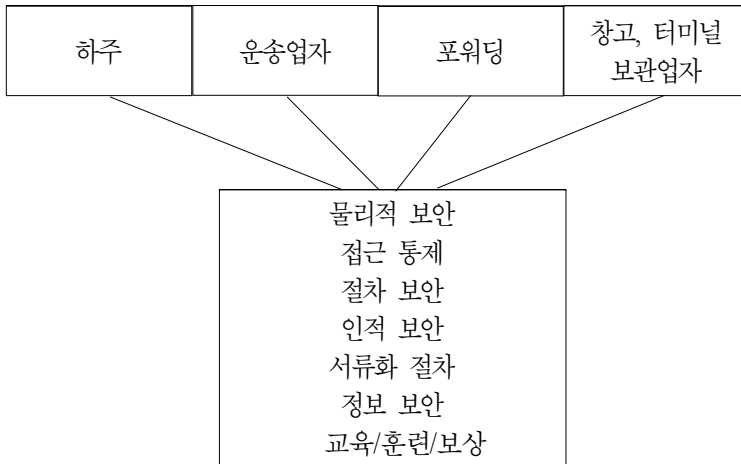
〈표 4-8〉 운송주선회사의 특별요건

항목	특별요건
접근 통제	- 시설의 불법접근 금지 - 통제는 다음 사항을 포함 • 고용자, 방문자, 사업관계자의 식별에 실패하지 않는 시스템 • 비승인, 미확인 인물에 대한 응대 절차
문서화 과정	- 회사는 제공된 문서의 확인을 위하여 최선을 다해야 하며, 화물의 교체, 손실 또는 잘못된 정보의 도입을 막기 위하여 감독성을 높여야 함 • 화주 및 위탁자 이름, 주소, 제 1, 2 통지서, 기술서, 중량, 수량, 화물측정 용기(박스, carton 등)의 수신 정보의 정확성 유지 • 화물의 부족 및 잉여에 관한 기록, 보고, 조사 • 반입 및 반출 화물의 이동 추적 • 컴퓨터 접근 및 정보 보호
절차 보안	- 회사가 감지하거나 의심하는 비정상적이거나 불법행위에 대한 대응 절차
문서화 절차	- 회사는 적화 목록, 송장 및 운송관련 서류의 완결성, 감독성, 정확성 및 제출 시간을 확인
인적보안	- 회사는 고용평등 및 개인정보보호에 관한 법률을 충분히 고려해서 장래 고용인에 대한 점검, 신청서 검증을 위한 내부 절차를 마련해야 함 - 내부 절차는 고용인의 이력 확인 및 특정 고용인의 관련 기능의 신뢰성에 대한 조사를 포함
정보보안	공급망 상에서 정보전달 절차는 확실해야
승인된 화물흐름 조항 (Secure freight flow provisions)	- 회사는 SO가 아닌 운영자가 제공한 화물을 확실할 수 있도록 검사하여 SO의 화물 수준으로 향상시켜야 함 - 만약 검사가 시행되지 않거나 화물이 승인된 공급망의 “신속 조치” 부분의 화물로 판단되지 않는다면 거절
교육 및 훈련 인식	- 예상되는 보안 위협 인식, 제품 무결성 유지 및 비권한자의 접근 한계 등이 포함된 보안 인식 프로그램을 고용자에게 제공 - 이런 프로그램은 보안 통제에 고용자의 적극적 참여를 강화하며 다음을 제공 • 적극적 고용자의 보안통제 참여에 관한 인식 • 문서 위조 및 컴퓨터 보안 통제 교육

〈표 4-9〉 창고 · 보관시설 · 육상터미널(내륙항만 포함) 운영자의 특별요건

항목	특별요건
물리적 보안	- 모든 건물과 재산이 불법진입 · 침입으로부터 보호될 것 - 다음 사항을 포함 • 내외부 문, 창문, 담장 등의 잠금장치 • 내부 및 주차장을 포함한 외부 시설의 조명 • 개인차량의 주차지역을 양적하 및 화물지역과 분리 • 내외부 통신시스템을 내부 보안인력 또는 지역 공안들과 연결
접근 통제	- 양적하 및 화물지역의 불법접근 금지 - 통제는 다음 사항을 포함 • 고용자, 방문자, 사업관계자의 식별에 실패하지 않는 시스템 • 비승인, 미확인 인물에 대한 응대 절차
절차 보안	- 기록되지 않은 물질이 창고, 보관 시설 또는 육상터미널(내륙 항만)에 반입되지 않게 적합하게 막아야 함 - 보안절차는 다음을 포함 • 위탁된 보안 담당자가 화물의 도입/이동을 감독 • 적화목록에 대하여 화물의 고유표식, 수량 파악 및 문서 작성 및 장비 점검 • 반입화물의 봉인 무결성 또는 다른 보안장치의 통제 • 반출화물의 봉인 및 다른 보안장치 시행 절차 • 부족 및 잉여의 검사 및 보고 • 회사가 감지하거나 의심하는 변칙 또는 불법행위 설명 절차 • 불법적 접근을 막기 위한 공개 또는 만재 용기의 적절한 보관
인적보안	- 회사는 고용평등 및 개인정보보호에 관한 법률을 충분히 고려해서 장래 고용인에 대한 점검, 신청서 검증을 위한 내부 절차를 마련해야 함 - 내부 절차는 고용인의 이력 확인 및 특정 고용인의 관련 기능의 신뢰성에 대한 조사를 포함
정보보안	공급망 상에서 정보전달 절차는 확실해야
승인된 화물흐름 조항 (Secure freight flow provisions)	- 회사는 SO가 아닌 운영자가 제공한 화물을 확실할 수 있도록 검사하여 SO의 화물 수준으로 향상시켜야 함 - 만약 검사가 시행되지 않거나 화물이 승인된 공급망의 “신속 조치” 부문의 화물로 판단되지 않는다면 거절
교육 및 훈련 인식	- 예상되는 보안 위험 인식, 제품 무결성 유지 및 비권한자의 접근 한계 등이 포함된 보안 인식 프로그램을 고용자에게 제공

〈그림 4-3〉 운영자의 최소한의 필요조건



위험평가는 승인받은 운영자 지위를 받고자 하는 회사의 일반적인 상황에 기초해서 단계별로 하여야 한다. 승인된 운영자의 자격은 3년간 유효하며, 이 규정의 최소한의 필요조건을 지속적으로 충족시키면 갱신된다(제8조).

〈표 4-10〉 위험평가

단계	평가내용
1단계	- 위협 유형의 확인 • 최근의 국내 및 국제 정세에 대한 실제뉴스 또는 테러리스트의 선전 • 시설 또는 공장에 대한 테러 공격 위협에 대한 보안 당국의 충고 • 테러리스트의 공격에 주요 표적이 되는 조직의 건물, 공장 또는 인물 • 테러위험이 높은 지역 인근에 위치함에 따른 부대적인 피해 가능성
2단계	무엇을 보호할 것인가? 특히 왜 그것이 테러 공격에 취약한가?
3단계	감당할 수 있는 수준으로 위험을 감소시키기 위해 무엇을 해야 하는가

⑤ 지위부여 절차

공급망보안의 책임당국은 승인된 운영자의 지위 부여에 대한 책임이 있다. 회원국은 모든 승인된 운영자의 등록부를 만들어야 하며, 등록부는 회원국의

책임당국과 책임기관, 그리고 유럽연합 집행위원회가 접근할 수 있어야 한다. 모든 승인된 운영자에게는 회원국의 국가 코드로 시작되는 ID가 부여된다. 회원국의 승인된 운영자의 지위부여와 관련하여 인정기관을 지정할 수 있다(제 10조). 공급망 보안을 위한 인정기관은 다음에 제시한 기준을 충족하고 있어야 한다.

- 기관과 고용인의 반부패 및 위반사항 기록
- 공급망 보안관련 측면에 있어서 전문성
- 운영 필수 지식을 포함한 공급망 운영에 적합한 지식
- 공급망 보안에 잠재적 영향을 미치는 운영관련 기타 보안에 적합한 지식
- 공급망 보안위험을 평가할 수 있는 능력
- 공급망 보안의 인적 전문성을 유지 및 향상할 수 있는 능력
- 지속적으로 인적 신뢰성을 감시할 수 있는 능력
- 보안에 민감한 물질에의 접근 및 불법적 노출을 회피할 수 있는 적합한 대책을 유지할 수 있는 능력
- 국가 및 국제적 입법 및 보안 필요조건과 관련된 지식
- 최근의 보안 위협과 양상에 관한 지식
- 무기, 위험 물질 및 장치에 관한 인식 및 감지할 수 있는 지식
- 공급망 보안을 위협하는 인물의 특성, 행동양상, 무차별성을 인식할 수 있는 지식
- 보안 대책을 회피하는데 사용되는 기술에 관한 지식
- 보안 및 감시 장비, 시스템, 운영한계에 관한 지식 등이 그것이다.

⑥ 자격의 철회 또는 정지

회원국은 공급망 보안을 위해 승인된 조직의 감독을 포함한 승인된 운영자 제도에 대하여 적절한 감시를 하여야 한다. 회원국은 승인된 운영자가 지위 부여시의 조건에 위반한 경우는 그 지위의 정지에 관한 규정을, 심각하게 또는 반복적으로 위반한 경우에는 그 지위의 취소에 관한 규정을 도입하여야 한다

(제9조 제1항). 승인된 운영자의 지위는 승인된 운영자 제도에 대한 회원국의 적절한 감독결과에 따라 취소될 수 있다. 이 자격이 취소되면 취소일로부터 2년 이내에는 재신청할 수 없고, 정지를 당한 경우는 공급망 보안의 책임당국이 위반사항의 시정에 만족하면 해제된다.

⑦ 이행 및 부합 점검

회원국은 공급망 보안을 위하여 승인된 조직의 감독을 포함하여 승인된 운영자 제도에 대하여 감독을 하여야 한다(제12조).

4) 시사점

EU는 선박 및 항만보안을 위해 국제 선박 및 항만시설 보안에 관한 규칙(ISPS Code)에서 규정하는 사항을 수용하고, 특히 권고사항(Part B)도 강제화하는 등 보안조치를 강화하고 있다. 또한 지난 8월 10일 영국에서 있었던 영국-미국 노선의 항공기를 액체폭약으로 폭파하려던 시도 이후 모든 액체의 기내 반입을 엄격히 통제하는 신 항공보안규정을 적용하고 있다. 이와 같이 선박 및 항만과 항공분야는 높은 수준의 보안을 유지하고 있다. 그러나 항공분야와 해상 및 항만분야의 보안조치들이 만족스럽게 이행되고, 인적 실수가 제거된다고 하더라도 그것은 전체 물류운송체계(공급망)의 특정분야에 대한 보안이 확보되는 것에 불과하다. 따라서 EU는 전 운송구간의 물류보안을 강화방안을 검토하였다.

예상되는 테러리스트의 공격으로부터 전 유럽의 화물운송의 보호를 강화하기 위해 EU 집행위원회가 설정한 목표는 다음과 같다. 첫째는 자유무역의 흐름을 방해하지 않고, 공급망에 따른 보안을 강화한다는 것으로 보안수준과 자유무역의 흐름 간의 균형관계 유지이다. 둘째는 최저보안요건을 충족하는 보안 체제 구축이다. 전 공급망에서 통제된 영역에서 운영되는 항공 및 해상운송과 같이 강력한 보안수준을 구축할 수 없으므로 단일의 포괄적인 보안운영체계

설립보다는 현실적이라는 이유에서다. 마지막으로 이러한 체제 구축에 있어서 유럽연합 및 각국 차원에서 불필요한 행정절차나 부담을 피하는 것을 목표로 하고 있다. 이러한 EU의 목표는 우리나라의 보안체제 도입시 타산지석으로 삼을 만하다. 우리나라 해상운송분야나 항공분야의 보안은 높은 수준이지만 그 이외의 운송구간 운영자들은 보안관리를 하지 않거나 시작단계이다. 따라서 공급망 전반에 단일 수준의 보안체계를 구축하기는 힘들기 때문에 최저 보안요건을 만족시키는 체제를 구축하여야 한다.

또한 EU 공급망 보안체계의 핵심은 관세당국의 공인 경제운영자와 같이 민간을 공급망 보안시스템에 자발적으로 참여시키는 승인된 운영자 제도(secure operator scheme)의 도입이다. 육상운송에는 아주 다양한 문화와 영업형태를 가진 다국적 기업에서부터 영세서비스회사에 이르기까지 약 50만개 이상의 회사가 운송 및 부대서비스에 관련되어 있어 정부 또는 제3자의 감시·감독방식에 의존하는 보안체제 구축은 그 실효성을 거두기 어렵다. 따라서 공급망 보안관리체제는 그 운영자의 참여 및 책임하에 운영하는 체제로 구축되어야 한다.

3. 일본의 물류보안제도⁷¹⁾

1) 부문별 물류보안제도

(1) 철도 부문

일본은 섬나라이므로 철도는 전적으로 국내수송만을 담당하고 있다. 운수정책연구소 자료에 따르면,⁷²⁾ 일본의 철도영업망은 약 27,383Km(2003년), 여객운송량은 약 3억 850만명, 화물수송량은 약 228억 톤Km로, 화물수송이 주종인 다른 나라와는 달리 여객 중심의 고밀도 수송이 특징이다.

71) 이 부문은 해외 협동연구 사업의 하나로, 일본의 이카와 테츠오(IMOS)가 집필하였음.

72) 재단법인 일본 운수정책연구소, “수치로 보는 철도,” 2005년 판.

일본 철도의 운영 주체는 JR, 지방공공단체, 민간철도, 제3섹터의 4개로 구분되고 있다. 철도운송 주체인 JR은 1987년의 국철개혁 이전에는 전국일체의 국유 조직이었으나 개혁 조치에 따라 6개의 여객 회사와 1개 화물회사로 민영화, 분할되어 현재에 이르고 있다. JR 여객회사는 국유철도시대의 철도망을 지역적으로 분할한 것으로, 간선 수송과 도시주변 수송을 담당하고 있다. 민간철도는 주로 도시 주변의 근거리 수송을 담당하고 있다. JR과 민간 철도의 수송량 비율은 2:1 정도이다.

일본 철도의 여객 수송량은 2,400만명/일, 화물 수송량은 103천톤/일로 국내 수송의 대동맥이나 현재의 보안대책은 그 규모에 비해 미약한 실정이다. 국내 외에서 진행되고 있는 물류보안 추세를 고려, 철도 경찰대나 승무원 등에 의한 차량 내 순찰의 증강과 승객에 대한 주의 환기, 역 구내에 경찰관 배치 등의 업무를 시행하고 있으나 공항에서와 같은 승객 개인별 수하물 검사 등은 전혀 없다. 근본적인 보안대책은 그 이용 규모나 형태로 보아 상당히 곤란한 것이 오늘날 일본의 실정이다.

(2) 항공 부문

항공업계의 보안대책은 다른 공공 교통기관에 비해 가장 발전된 것으로 평가되고 있다. 공항은 해외로 통하는 주요 관문으로 그 동안 비행기 납치 대책 등에 따라 보안 대책이 비교적 양호한 실정이다.

그러나 이에 인한 과제도 적지 않다. 승객 개인의 수하물, 항공화물의 검사 강화는 물론 승객에 대한 보안과 관련해 혐의자에 대한 검문, 철저한 지문채취와 같은 문제가 현안으로 부각되어 있다. 항공화물에 있어서는 항공회사뿐 아니라 화물 운송을 의뢰하는 하주, 화물 혼재업자의 보안대책계획 수립 참여, 국가에 의한 보안대책비용 조성, 이용자 부담의 사회적 합의 도출 등과 같은 문제가 여전히 걸림돌로 남아 있다.

(3) 해운 부문

해운업계는 최근 보안대책 수립에서 핵심이 되고 있다. 그러나 일본의 경우 특히 물류 부문에서 해운이 일본 무역량의 99% 이상을 운송하는 등 차지하는 비중이 거의 절대적임에도 불구하고, 이 부문에 대한 보안대책이 너무나 빈약한 것이 사실이다.

국제적으로 해운 부문은 9·11 테러 영향으로 IMO가 2001년 11월 제22회 정기총회에서 선박 및 항만시설의 보안에 관한 새로운 조치를, 2002년 12월의 1974년 해상인명안전조약(SOLAS) 체결국 회의(외교회의)에서 기존 협약 개정안을 전원일치로 채택하였다. 이와 같이 1년이 조금 넘는 짧은 기간 동안 이 같은 조치가 이루어진 것은 사태의 중요성과 함께 보안상의 사건이나 위협으로부터 세계 해운을 지키고자 하는 의지의 표현이라 할 수 있다. 이 조약 개정안은 주지하는 바와 같이 2004년 7월 1일에 국제적으로 발효되었다.

이 개정에 따라 새롭게 도입된 ISPS 코드⁷³⁾는 국제무역에 사용되는 선박(국제항해선박), 또는 항만시설에 관한 사건에 대해 보안에 관한 위협을 발견하여 예방조치를 강구하기 위해 체결국 정부, 회사의 보안직원(CSO : Company Security Officer), 선박의 보안직원(SSO : Ship Security Officer), 항만시설의 보안직원(PFSO : Port Facility Security Officer) 등 관계자 각각의 역할 및 임무를 명확히 하여 국제적인 틀을 구축하는 것을 기본 목적으로 하고 있다.

선박은 그 관련시설(접안 부두 시설 등)을 포함하여 항상 보안상의 위협에 노출되어 있다. 그리고 이러한 위협은 최근 들어 더욱 다양하고 심각해졌다. 일본뿐만 아니라 전 세계를 이동하는 국제항해선박은 테러의 주요 대상이 되고 있다. 이에 따라 위험물을 수송하는 국제항해선박이 테러의 표적이 될 수 있다는 것이 전문가들의 지배적인 시각이다. 개정 SOLAS 조약은 항만시설을 포함한 해상의 자주경비체제 정비를 기본 개념으로 하고 있다. 과거의 해상보안사건이나 데위 만드림(Dewi Mandrim) 호 사건에서 나타난 바와 같이 일

73) 일본에서는 ISPS Code를 자주경비제도라고 부르고 있음.

본의 경우 말라카 해협의 해적 문제가 보안과 관련해 주요 현안으로 등장하였다. 특히 최근 들어 해적이나 테러리스트 사이의 경계가 모호해짐에 따라 선박의 자주경비체제를 테러대책과 해적대책으로 나누어 고찰할 필요가 없는 시대가 되었다.

또한 일본은 미국과 CSI 협정을 체결하고, 2003년 3월부터 요코하마 항, 2004년 5월부터 도쿄 항, 같은 해 8월부터 나고야 항, 고베 항에서 미국행 컨테이너 화물에 대한 보안검색을 실시하고 있다. 이와 함께 미국이 도입한 C-TPAT (Customs-Trade Partnership Against Terrorism)에 대해서도 2002년 4월부터 일본의 제조기업이나 해운업체와 같은 사업자들도 참여하고 있다. 이처럼 해운 부문에서는 민관이 함께 다각적으로 빠른 속도로 물류보안제도를 도입·시행하고 있어 한편으로는 물류보안이 강화되고 있으나 그에 따른 부담 또한 커지고 있는 것도 사실이다.

2) 해운업계의 보안대책과 과제

(1) 정부 당국의 테러 대책

① SOLAS 조약 이행 문제

해상테러에 대응하는 이른바 개정 SOLAS 조약의 영향으로 일본은 국내법으로 ‘국제항해선박 및 국제항만시설의 보안 확보 등에 관한 법률(이하 국내법이라고 함)’을 제정하고, 2004년 4월부터 시행하고 있다. 이 법률은 주로 국토교통성에서 집행하고 있는데, 관계당국이 담당하고 있는 테러대응상황은 다음과 같다.

가. 해사국

해사국은 국제항해선박에 관한 사항을 관장하고 하는데, 주로 항만국 통제업무(PSC)를 담당하고 있다. 또한 국내법에서는 선박에 배치해야 될 SSO(선

박보안담당자)의 양성기관으로 일본 해기대학교를 지정하였다.⁷⁴⁾ IMO는 각 보안직원 (CSO, SSO, PFSO)의 양성 코스를 도입·운영하도록 요구하고 있는데, 교육과정의 약 30%는 테러에 관한 것(상정 위협, 무기)을 포함하도록 규정하고 있다. 일본은 보안훈련, 실습, 연습에 관한 사항은 전문가나 전직 해상보안관 등 외부 전문가를 활용하여 실시하고 있다.

나. 항만국

항만국은 해사국과 달리 국제항만시설 정비에 관한 업무를 담당하고 있다. 항만국은 개정 SOLAS 조약, 국제항해선박 및 국제항만시설의 보안 확보 등에 관한 법률(약칭 : 국제선박 및 항만보안법)에 따라 국제항만시설 관리자 등이 신청한 부두 보안규정 및 수역보안규정(조약의 항만시설 보안계획)에 관한 승인업무를 수행하고 있다. 항만국에 의하면, 2005년 7월 1일 기준으로 국제항만 126개소, 국제 항만시설 1,948개소가 보안규정에 따른 승인을 받은 것으로 나타났다. 또한 항만국은 항만시설에 있어서의 경계강화로서 다음 조치를 실시하고 있다.

- 순회경비 강화, 항만시설의 내외 감시
- 출입관리 실시
- 제한구역 설정 (펜스 설치), 보안 조명시설 및 감시 카메라 등 설치
- 화물 취급을 관리
- 항만시설의 보안관리자 선임
- 각 국제항만에 국토교통성, 해상보안청, 세관 등을 구성원으로 하는 항만보안위원회를 설치하고, 관계기관의 연계를 강화하고 있다.

다. 해상보안청

선박보안정보에 관한 것과 해상보안청법(제2조)에 따라 전반적인 해상의 치

74) 일본의 경우 CSO, PFSO에 대해서는 법적으로 양성기관이 존재하지 않은 실정임.

안 유지, 범죄 예방, 진압 등에 관한 업무를 처리하고 있다. 특히 외국에서 처음 일본에 입항하는 국제항해선박은 24시간 전까지 국내법 시행규정에서 정한 25개 항목의 선박보안정보를 해상보안청에 통보해야 한다. 해상보안청은 통보 받은 선박보안정보 등을 토대로 그 선박에 대한 출입검사의 시행여부를 판단한다. 일본은 이 같은 업무를 보다 효과적으로 수행하기 위해 2005년도 예산에서 자폭(自爆) 보트 대책용 경비정과 특수부대 수송용의 대형 헬리콥터를 도입하기로 하는 등 보안 및 테러 장비를 더욱 확충하고 있다. 이 밖에 해상보안청이 ‘테러대처, 수상한 선박 대처의 사전방지 대책’에서 제시한 보안 대책은 다음과 같다.

- i) 순시선정, 항공기에 의한 감시 : 항만, 항로부근에서의 철저한 감시경계 등
- ii) 외국선박에 대한 출입 검사 등에 의한 해상 경계 : 정보 분석에 근거한 요주의선박에 대한 철저한 출입검사 및 감시철저
- iii) 임해부의 중점 경비대상 시설의 경비 : 전국의 원자력발전소 전면 해역에 순시함정 상시 배치 등
- iv) 해사관계자 등에 의한 철저한 자주 경계 : 철저한 자주경비의 지도 및 수상한 자에 대한 정보제공 등을 의뢰
- v) 국제선박, 항만법(개정 SOLAS 조약)의 운용 : 외국에서 일본에 입항하는 모든 선박에 대한 보안조치 실시상황의 확인 등 엄격한 입항규제
- vi) 항만의 위기관리체계 강화 : 5대항(도쿄, 요코하마, 나고야, 오사카, 고베)에 위기관리관 설치 등
- vii) 대량파괴병기 등의 수송 방지·단속(PSI) : 관계국과의 연계 강화, 국내 법령에 의한 엄격한 단속
- viii) 테러와 관련한 적절한 정보수집활동 등이 해상보안청이 현재 테러 방지를 위해 역점을 두고 실시하고 있는 사업이다.

② 기타 관계기관

가. 내각

내각관방(내각대변인 및 국무조정실의 기능)의 홈페이지에 의하면 내각은 국가 안전에 관계되는 사항 및 국민의 생명, 신체 또는 재산에 중대한 피해가 발생, 혹은 발생할 위험이 있는 긴급사태에 대한 대처에 관련된 중요 정책의 기획, 입안 및 종합조정업무를 수행하고 있다. 최근에는 테러대책 특별조치법과 유사관련법안 등의 중요시책 추진에 중심적인 역할을 하고 있다.

또한 일본은 대규모의 자연재해, 비행기 납치·테러 등의 중대사건, 항공기·원자력 사고 등 중대사고, 무장 간첩선 사건 등 다양한 긴급사태 발생에 대비하는 한편, 위기관리를 위한 매뉴얼의 정비와 훈련을 행함과 동시에 관계기관의 상호 연계체제를 강화하고 있다. 긴급사태가 실제로 발생한 경우에는 총리대신의 관저에 있는 위기관리센터에서 초동 대처하도록 지침이 마련돼 있다.

이 같은 상황을 해상으로 한정해 보면, 관방장관과 부 관방장관 밑에 위기관리감을 설치하고, 위기 관리감을 장으로 하는 ‘공항 및 항만 해상 위기관리팀’을 신설하였다. 또한 5대 항만(도쿄, 요코하마, 나고야, 오사카, 고베)에 위기관리관을 설치(각 해상보안(감)부장을 임명)하였으며, 그 외의 항만에는 경찰서장 또는 해상보안부처장을 위기관리 담당관으로 배치하는 등 핫라인을 구축하고 있다.

2005년에는 위험성이 높은 선박을 대상으로, 민관의 전문가로 구성된 ‘해상 테러에 의한 선박으로부터의 위험물 유출 피해 및 예측에 관한 조사검토위원회’를 설치하는 한편, 이 위원회의 의견을 들어가면서 현지조사와 관계자의 의견 수렴을 병행, 필요한 물류보안조치를 마련하고 있다.

나. 방위청

한편, 대테러와 관련하여 방위청과 자위대에게는 영역 경비라는 새로운 임

무가 부여되었다. 영역경비란, 평상시에 [영공-영해-영토의 보전]임무 뿐만 아니라 [비상] 사태 발생시 [영공-영해-영토의 보전] 임무까지 수행하는 것을 말한다. 즉 일본은 자위대법을 일부 개정해 [유사]에 이르기 전의 평시부터 비상 시까지를 포함해 자위대가 필요한 국토보전임무를 수행하도록 하였다.

이 같은 자위대의 새로운 임무 이행은 전후의 자위대의 존재를 근본부터 전환하는 것으로, 당면의 주 임무가 [유사시에 출동하는 군대]에서 [평시-비상시에 출동하는 군대]로, 즉 경찰기관을 대신하여 [국가의 위기관리]를 군사적으로 맡는 실력조직으로 이행되고 있다는 점이다. 이는 유사법제의 정비와 연계한 조치이다.

일본 정부는 영역경비에 관한 자위대법 개정 근거해 2003년 11월 2일에 ‘대규모 테러 등의 위협이 있는 경우의 정부의 대처에 관하여(각의결정)’라는 문서를 발표하였다. 이 문서에는 9·11 참사와 같은 테러, ‘소총, 기관총, 포, 화학병기, 생물병기 등의 살상력이 강한 무기를 소지한 무장 공작원 등에 의한 파괴활동, 기타 이에 유사한 사건이 일본에서 발생할 위험이 있고, 일반 경찰력으로는 대응할 수 없는 사태’에 대해 내각 총리대신을 본부장으로 하는 대책 본부를 설치하도록 규정하고 있다.

또한 사태가 긴박하여 치안출동명령의 발령이 예측되는 경우에는 대책본부의 산하에 방위청을 중심으로 사전에 치안출동명령의 발령에 관계되는 대처방침의 검토, 자위대와 경찰간의 역할분담 및 연계 확인, 필요한 정보의 공유 등에 관하여 상호 최대한 협력하는 한편, 내각 총리대신이 치안출동을 명한 때에는 신속하고 강력한 대처를 행할 수 있는 태세를 마련하는 것을 주요내용으로 담고 있다.

(2) 해운업계의 실태와 과제

2006년 12월 기준으로 개정 SOLAS 조약과 ISPS 코드가 발효된 지 2년이 넘었다. 이 같은 제도는 세계적으로도 예를 찾아볼 수 없도록 신속하게 발효된 것이 특징이다. 그러나 일본의 경우 다음과 같은 사정으로 진정한 물류보안 체

제가 구축되어 있지 않은 실정이다. i) 무기를 자유롭게 소지할 수 있는 사회가 아닌 점, ii) 전후 60년 이상 평화 체제가 지속되고 있는 점, iii) 국제테러의 거점이 적고, 국제테러가 발생하지 않은 점, iv) 항만시설을 포함한 해상의 자주 경비체제 라인 구축을 각 감독관청이 분야별로 추진하고 있는 점, v) 각 보안 직원 양성의 인적 인프라인 해사보안 경험에 있는 자가 적은 점 등이 그 이유인 것으로 풀이되고 있다.

또한 일본의 경우 국제선박 보안증서(ISSC) 취득과 같은 법률 절차는 정비되어 있으나 CSO, SSO, PFSO의 지식 및 기능의 향상, 유지, 선박보안계획(SSP)의 개정, 훈련, 연습의 기획 및 입안, 조정, 실시, 평가라는 이른바 소프트웨어의 과제 등이 산적해 있다. 특히 회사의 보안감사, 테러 대응 훈련, 연습 매뉴얼 작성 등에 대해서는 거의 이루어지고 있지 않다. 이 같은 문제가 발생하고 있는 것은 근본적으로 CSO가 육성되어 있지 않는 것이 첫 번째 문제인데, 일본에서 진정한 CSO가 육성되기까지는 10~20년 정도 소요될 것이라는 의견이 지배적이다.

ISPS 코드는 바람직한 자주경비체제이나 선사 등 관련기관이 적극 대처하거나 활용하지 않는 경우 그 효용성이 크게 저하되는 것이 큰 문제점으로 지적되고 있다. 일본은 아직도 인력부족과 보안의식이 결여되어 있어 선사 중에는 “어떤 처분이나 피해가 발생하지 않으면 적극적으로 대응하지 않아도 된다”라는 의식이 만연해 있는 실정이다. 일상적이긴 하지만, 중간검사를 맞이한 2006, 2007년에 선사와 관계당국의 대응이 주목되는 이유가 바로 여기에 있다. 선사의 최고 책임자부터 ISPS 체제의 확립이 곧 조직의 위기 관리라고 인식하지 않는다면, 진정한 자주경비체제는 구축되지 않는다. 일본에서 진정한 의미의 ISPS 체제가 구축되는 것은 회사보안담당자(CSO)를 포함한 회사의 보안의식이 고양된 후인데, 앞으로 10년 이상은 걸릴 것으로 판단된다.

3) 향후 일본의 물류보안 대책

미국은 2001년 9월 11일 동시 다발적인 테러가 발생함에 따라 국제 테러 네트워크 전체를 괴멸시키기 위한 테러와의 전쟁을 선언하였다. 또 테러지원국가로 지목한 국가는 대부분 대량살상무기의 개발을 적극적으로 추진하고 있다는 전제 하에 특히 이라크와 북한에 대하여는 과거보다는 훨씬 엄정하게 대처한다는 방침을 세웠다.

직접적으로는 아프가니스탄의 탈레반 및 알 카에다 거점에 대한 공격이나 대 이라크 전쟁을 대표적인 사례로 들 수 있다. 그 이외에도 미국은 테러로부터 자국의 국민과 국토를 보호하기 위해 연안 경비대를 포함한 22개의 보안 및 안전 담당행정기관을 통합한 국토보안부를 설치하는 등 광범위한 물류보안 정책을 입안, 시행하고 있다.

특히 미국은 자국의 보안기준을 SOLAS 조약의 개정 등과 같은 방법으로 전 계적으로 적용하는 글로벌 기준화하는 한편, 외국항만에서의 테러대책의 유효성을 평가하여 유효한 테러대책을 강구하고 있지 않은 항만에서 화물을 적재한 선박의 입항을 거부할 수 있는 등의 규정을 포함한 해운보안법에 포함하는 등 세계적인 차원에서 테러리스트의 움직임을 봉쇄하기 위한 모든 전략을 국제적·국내적으로 추진하고 있다.

미국의 이 같은 물류보안조치 강화에 따라 일본선박 또한 미국정부로부터 입항거부조치⁷⁵⁾를 당하는 사례가 발생하고 있다. 이에 그치지 않고, 입항허가를 얻기 위한 비용, 시간 등의 부담이 증가할 것이 예상되고 있으며, 이 역시 일본해운업계에 큰 영향을 미칠 것으로 우려된다. 일본항만 및 주변해역에서도 지속적으로 긴장이 고조되고 있고, 북한 정세와 국제 테러조직에 의한 테러의 가능성이 높아지고 있다는 점을 고려할 때 미국 등의 테러대책에 관한 동향도 참고하는 한편, 민관이 연계하여 보다 면밀한 물류보안대책 마련이 시급한 실

75) 일본의 경우 2004년 7월 1일~2006년 5월까지 미국 내의 선박 항만국 통제에서 160척이 경고 또는 주의 등과 같은 처분을 받았음.

정이다. 미국의 동맹국이기도 하고 무역 상대국이기도 한 일본의 해운업계는 그야말로 격동의 시대를 맞이하고 있다.

4) 시사점

한편, 일본의 물류보안제도는 기본적으로 IMO의 ISPS Code를 근간으로 하고 있다. 그리고 중국과 같이 미국과 CSI 협정을 체결, 동경항만과 고베, 나고야 항만에서 미국행 컨테이너 화물에 대한 사전 검색제도를 시행하고 있으나 아직은 미온적으로 대처하고 있는 것으로 나타났다. 연구진이 지난 9월 일본 항만 및 물류보안 전문가 등을 대상으로 인터뷰한 바에 따르면, 일본의 4개 항만에는 컨테이너 검색 장비로 X선, 적외선 검색기가 설치되어 있는 것 이외에는 다른 나라에 비해 선도적으로 물류보안 활동에 나서지는 않는 것으로 분석되었다.

특히 일본의 경우 정부 및 민간부문에서 화물 검색을 포함한 물류 보안에 대한 관심이 매우 저조한 것으로 드러났다. 또한 컨테이너 화물의 전자 봉인에 대해서 일본은 아직 기본적인 인식단계에 머물고 있으며, 현재 단계에서는 중요하다고 인식하지 않고 있는 실정이다.

또한 물류보안에 대한 일본의 입장은 현재 추진·논의되는 내용이 가장 좋은 방법인지 여부에 대한 확신이 없다는 인식이 강하며, 화주나 미국이 주도하는 것이고 선사, 항만은 주역이 아니기에 따라가는 입장이라는 견해를 견지하고 있다. 다만, 일본은 자국으로 들어오는 컨테이너 화물에 대한 위험성 검사 등에 대해서 담당부처인 재무성은 관심이 없으나 국제적인 동향을 반영, 화물 검색기 설치를 확대하는 정책을 추진하고 있다. 결론적으로 일본의 경우 현재 국제적으로 시행되고 있는 물류보안제도 가운데, 최소한의 기준과 요건을 이행하고 있는 것으로 보이며, 정부와 민간 부문의 인식이 낮은 수준인 것으로 평가되고 있다.

4. 중국의 물류보안 제도⁷⁶⁾

1) 부문별 물류보안제도

(1) 해운·항만 부문

중국은 항만 및 육상 부문의 보안제도 강화에 앞서 테러 범죄에 대한 처벌을 강화하기 위해 기존 법률을 개정하는 등 필요한 조치를 마련하고 있다. 2001년 12월 제9차 전국 인민 대표자 대회(이하 전인대) 상무위원회에서 형법 수정안을 통해 테러범죄 관련 17개 죄명을 추가하는 등 처벌을 강화하고 있다. 이와 함께 전인대는 통일적인 반 테러 법률을 제정하는 방안을 추진하고 있다. 이 법률은 반테러 기본 원칙, 반 테러 기관 및 주요 직책, 테러 범죄 행위의 확정, 테러 범죄행위의 예방책 등을 규정함으로써 사법기관과 행정기관에 법률적 근거를 제공하게 된다. 중국은 2005년 9월에 개최된 제22차 세계법률대회에서 현재 제정을 추진하는 반테러법의 주요 내용이 확정되었다고 발표하였다.⁷⁷⁾

중국의 항만보안에 관한 제도는 일반적으로 항만법과 항만시설보안규칙에 명시되어 있다. 2002년부터 시행되고 있는 항만법(제4장)의 “항만안전 및 감독 관리”에서 항만보안에 관한 원칙을 두고 있는데, 항만 경영인과 항만행정 관리 부서가 항만 안전과 보안의 책임주체가 되는 것으로 규정하고 있다. 항만시설 보안규칙(港口设施保安规则)은 2003년 11월 중국 교통부가 개정 SOLAS 조약 XI-2와 국제선박 및 항만시설보안규칙(ISPS Code)을 이행하고, 항만보안업무를 강화하기 위해 제정한 법률이다. 이 규칙에는 보안등급, 보안평가, 보안 계획, 보안요원, 보안 선언서 보안교육과 훈련 및 연습 등에 관한 내용이 포함되어 있다. 중국은 이 법률을 효과적으로 시행하기 위해 i) 선박보안규칙을 공포하고, ii) 항만시설 보안료 징수에 관한 통지를 발하는 등 필요한 조치를 취하고 있다. 해운 부

76) 이 부문은 해의 협동연구 사업의 하나로 중국의 Ru Yihong 교수(북경 교통대학교)가 집필하였음.

77) 중국 반테러법의 주요 내용과 반테러 협력 구축, <http://www.police.com.cn>.

문에서는 국제선박 및 항만시설보안규칙이 물류보안에 관한 중국의 기본 법률이다.

한편, 중국의 해운·항만의 보안제도를 담당하는 부서는 해운과 항만 부문으로 각각 구분되어 있다. 전자의 경우 교통부 수운사(해운국)에서 담당하는 반면, 후자는 지방으로 이관되어 처리되고 있다. 즉, 2003년 항만관리체제 개혁에 따라 항만관리권이 지방정부로 이관되고, 행정과 기업이 분리되었다. 신규 설립된 항만행정 관리기관(항만관리국 등)은 항만관리 주체역할을 수행하고, 기존 교통부의 물류안전에 대한 관리기능도 지방항만 행정기관으로 이관되었으며, 교통부는 정책의 제정 등 거시적인 항만관리업무만을 담당하게 되었다.

중국 교통부는 2004년에 담당 차관을 팀장으로 하고, 각국 국장을 구성원으로 하는 SOLAS 협약 해상보안이행 협력팀을 구성하였다. 또한 산하에 선박 및 항만 이행팀을 두었다. 각급 교통(항만) 주관기관과 항만행정 관리기관들도 이에 상응한 항만시설 보안팀을 구성하고, 구성원을 교통부에 보고·등록하도록 하였다. 또한 교통부는 수운과학연구소와 중국 선급에게 권한을 위임하여 인증보안조직(RSO)으로서 항만시설과 선박보안에 대한 기술서비스를 제공하도록 하고 있다.

(2) 육상운송 부문

도로 및 철도 등 육상운송 부문에 대한 보안제도는 아직 국제적으로 명시적인 규정이 나오지 않았기 때문에 유사 사태 발생에 따른 국가 대응방안 수립에 초점을 맞춘 보안 및 안전제도 시행이 주가 되고 있다. 먼저 중국은 도로 부문의 보안을 확보하기 위해 2006년 1월에 돌발 사태에 관한 국가 전체적인 긴급대응방안을 마련하였다.

이 대응방안은 각종 돌발 사태를 여러 등급으로 분류하고, 대응방안을 명확히 하는 한편, 초대형 돌발 공공사태에 대응하는 조직체계와 업무체제 등을 포함하고 있는 것이 특징이다. 철도 부문에서도 철도 운행사고에 대한 국가긴급 대응방안을 수립·시행하고 있다. 이 방안은 철도 운행사고로 인한 인원 사망

과 부상, 재산의 손실, 공공안전에 미치는 영향을 예방 및 최소화하고, 사고를 적시에 처리함으로써 철도운송의 정상적인 질서를 회복하는 데 그 목적이 있다. 미국이 항만보안법(SAFE Act)을 제정하면서 테러 이후의 교역 정상화 계획을 수립하도록 한 것과 맥을 같이 하는 제도로 평가되고 있다.

2) 물류보안 시설·장비 개발

(1) 컨테이너 화물 검색기

중국은 화물 공급망의 안전보장을 목적으로 5년 전부터 무삽입(無挿入) 화물 검색기를 주요 항만에서 광범위하게 설치하기 시작하였다. 현재 중국세관은 연해 및 내륙 항만에 55개 컨테이너 화물 검색 시스템을 설치·운영하고 있다. 또한 중국세관 통제기술 연구센터를 설립하여 주로 세관 인원의 검사기술 교육과 위험식별 시스템, 위험관리, 위험요인 분석 등을 수행하고 있다.

이에 앞서 칭화통광위이스(清華同方威視, Nuctech)사는 1998년에 세관당국과 협력 시스템을 구축, 'H986 프로젝트'를 수행하였다. 이 사업은 1998년 6월 중국 국무원의 허가를 얻은 대형 컨테이너 화물 검색 설비 및 그 보조시스템의 개발에 관한 사업으로, 첨단 과학기술을 활용하여 수출입 컨테이너 화물에 대한 X레이 검사를 통하여 실제화물과 신고화물의 일치여부를 확인하는데 목적을 두고 있다.

이와 관련하여 Nuctech 이미 40여 개 대형 컨테이너 및 차량 검사시스템을 제공하였다. 또한 Nuctech는 철도부, 병기산업부, 우주항공산업부 등과 협력관계를 구축하는 한편, 대외적으로는 제품을 유럽, 미주, 대양주, 아시아, 아프리카 등 10여 개 국가 및 지역에 수출하였다. 1997년 7월에 설립된 Nuctech는 칭화대학 산하 하이테크기업으로, 복사영상(輻射映像) 기술 분야에 있어 수십 년 간의 연구경험과 기술노하우를 보유하고 있다. 특히 핵심기술에 대한 지적재산권을 보유하고, 수십 여 개의 국내외 기술특허를 취득하였다. 현재 중국은 프랑스, 독일, 영국에 이어 세계에서 네 번째로 대형 컨테이너 화물 검색 기술

을 보유한 국가로 떠올랐다.⁷⁸⁾

(2) 세관 위험 화물 식별 시스템⁷⁹⁾

2005년 중국의 컨테이너 물동량은 전년대비 6.3% 증가한 5,730만 TEU에 이르렀다. 중국 세관에서 접수한 통관 신고서류도 391만 건에 달하고 있다. 중국 세관은 물동량이 급증함에 따라 위험 화물 식별시스템을 구축하고 있다. 이 시스템은 전자통관 신고정보, 전략정보, 자동거래 데이터, 세관인원의 개인경험의 누적정보 등을 포함한 종합적인 위험요인을 수집 및 선별할 수 있는 설비이다. 특히 이 시스템은 위험지수를 확정하고, 위험 발생이 우려되는 통관신고서와 선적 명세서를 선별하여 해당 분석관에게 전송함으로써 효과적으로 위험 화물과 컨테이너를 식별할 수 있도록 설계되어 있다.

(3) 스마트 컨테이너 연구

컨테이너 운송에 있어 2대 과제는 적시 수송(Just-in-time)과 물류보안의 확보라 할 수 있다. 오늘날의 컨테이너 운송은 실시간과 편리한 관리 및 안전성을 요구하고 있기 때문이다. 예컨대 컨테이너 운송시스템에 어떠한 결함이 있다면 운송의 연속성과 실시간 추적에 영향을 미치게 되어 중국적으로 글로벌 공급망 발전에 상당한 영향을 미치게 된다. 이에 따라 중국세관은 작업팀을 구성하여 Smart Box 표준에 대한 연구를 강화하고 있다. 또한 수출입 화물과 컨테이너의 안전요인이 위험 식별 시스템의 위험지수의 하나로 활용할 수 있도록 노력하고 있다.

(4) 위험물 물류관리 시스템

이 시스템은 중국 항톈(航天) 그룹은 갈릴레오 프로젝트에 참여하면서 도입

78) Nuctech사는 최근 세계에서 최초로 가속기 복사원을 이용한 차량탐재 이동식 컨테이너·차량 검색 시스템(Mobile Container/Vehicle Inspection System with a linear accelerator is radiation source)을 개발, 상용화하였음.

79) China Custom Targeting System(CCTS)

한 차량탑재 위성항법 위치시스템 장치에 메시지 통신시스템과 관련 소프트웨어를 집합하여 개발한 물류보안장비이다. 이 시스템은 위성 자동위치 선정, 다중 카메라를 이용한 동태 정보 수집, 메시지를 이용한 정보 피드백, 실시간 관리 등과 같은 기능을 보유하고 있으며, 현재 사고정보, 선로정보 등 서비스를 제공하고 있다. 중국의 국가 생산 안전 감독 관리국과 공안부 교통관리국은 공동으로 위험 화학물질을 운송하는 데 있어 이 시스템을 사용하도록 적극 권장하고 있다. 향후 위험물과 폭발물에 대한 운송관리와 통제를 강화하고, 제조기업의 책임을 강화하기 위해서는 차량과 터미널 등 주요 공공장소에서의 위험물 반입 금지제도를 도입하고 위험물과 금지화물에 대한 검사를 강화해야 한다는 것이 중국의 기본적인 시각이다.

3) 중국의 물류보안 과제

(1) 항만 물류 부문

중국의 경우 아직 물류보안제도가 초기단계에 있기 때문에 각 부문에서 여러 가지 문제점이 있는 것으로 파악되고 있다. 항만 부문과 육상 부문으로 구분해 문제점을 적시하면 다음과 같다.

항만부문에서는 첫째, 항만행정 관리체제 개혁이 불균형적으로 이루어지고 있고, 감독관리에 허점이 있다. 물류보안관리는 항만행정관리의 중요한 내용임에도 불구하고, 현재 일부 항만행정 관리기관은 체제의 불건전, 인원부족, 행정과 기업의 미 분리, 보안관리 직책의 불명확 등과 같은 문제점을 안고 있다.

둘째, 항만안전 및 보안관리 기능의 중첩문제가 심각하다. 선박과 항만시설의 안전업무는 선박, 선사, 항만경영자, 항만행정 관리기관 외에 국가의 해사, 교통, 수상운송, 공안, 세관, 국경수비 등 기관과 연관되어 있다. 일부 사항은 직접적으로 국가안전과 비밀업무와 연관된다. 이와 같이 많은 부처에 업무가 분산됨에 따라 정보소통의 어려움과 보안자원의 중복 및 낭비가 심각한 실정이다. 따라서 효과적인 선박 및 항만시설의 보안시스템을 구축하기 위해서는

우선적으로 각 기관간 업무관계를 명확히 하고, 원활한 정보 협력체제를 구축하는 한편, 보안 인력을 통합하는 것이 필요하다.

셋째, 항만시설 보안료 징수에 대한 항만기업의 참여가 미흡하다. 교통부와 국가발전개혁위원회는 2006년 6월 1일부터 항만시설 보안료를 징수하고, 징수기간을 3년으로 확정하였다. 그러나 실제 이행상황은 매우 만족스럽지 못한 실정이다. 현재 일부 항만에서만 항만시설 보안료를 징수하고 있고, 대부분 중소항만은 여전히 방관하고 있는 것으로 나타났다. 그 주요 원인은 항만보안에 대한 투자 증가로 항만경영 및 관리 비용이 크게 늘어날 것으로 우려하고 있기 때문이다. 이 밖에도 인근 항만간 치열한 경쟁과 업체간 조정 미흡 등도 문제점으로 지적되고 있다.

넷째, 항만보안 요원과 관련해서는 보안요원이 자주 변경되고 있고, 항만기업은 일반적으로 중간 간부를 보안요원으로 지정하고 있는데, 중간 간부의 권한, 즉 지휘명령권이 없다는 점이 물류보안의 효율성을 떨어뜨리는 요인으로 작용하고 있다. 한편, 이 같은 문제점을 개선하기 위해서는 다음과 같은 대책이 필요한 것으로 의견이 모아지고 있다.

(2) 육상 물류 부문

도로 부문에서는 첫째, 아직 물류보안(테러방지)을 전담하는 법률이나 법규가 제정되어 있지 않으며, 도로운송과 관련된 응급대책도 완벽하지 못한 실정이다. 둘째, 육상의 물류 보안을 확보하는데 필요한 교통관리 시스템의 지속적 개선도 필요하다. 현재까지 중국은 대규모 도로건설에 치중하고 있어 도로운송 안전과 관련된 교통관리시스템은 아직 비교적 낙후한 실정이며, 지능운송시스템은 베이징, 상하이, 선전 등 10개 도시에서만 운영되고 있다. 셋째, 철도부문에서는 테러방지 사전 경보시스템이 마련되어 있지 않다. 철도의 테러방지 특징과 규칙에 따라 투자를 확대하고, 선진적인 물류보안 기술 장비의 연구, 개발 및 도입을 추진해야 하나 아직 이 부문에 대해서는 관심을 기울이지 못하고 있는 실정이다.

4) 중국과 외국의 물류보안 협력

(1) SOLAS 협약과 ISPS 코드 이행

중국은 SOLAS 협약의 체약국으로 이 협약을 성실하게 이행하고 있다. 협약이 개정된 이후인 2003년에 국제 선박보안규칙과 항만시설 보안규칙을 제정하였다. 특히 항만시설 보안규칙은 국무원 교통주관기관, 성, 직할시의 교통담당기관과 항만행정 관리국의 항만시설에 대한 보안평가의 실시, 심사 및 비준절차를 명확히 하고, 각급 지방정부 주관기관과 항만시설 경영자, 항만시설 보안요원의 직책과 임무를 규정하고 있다. 교통부 수운사와 교통부 수운과학연구소는 이 규칙을 바탕으로 항만시설 보안지침을 마련하고, 항만시설보안평가보고서와 항만시설보안계획의 서식을 제공하는 등 협약 이행을 지원하였다.

또한 SOLAS 협약 수정안과 ISPS 규칙에 따라 중국 해사국은 중국 선급(CCS)에게 선박보안평가와 계획에 대한 확인 및 인증사항을 위임하는 등 선박의 보안 확보에도 적극 나서고 있다. 미국의 평가는 다음과 같다.

한편, 2006년 3월 미국 연안 경비대는 항만시설 보안업무와 관련해 중국을 방문하고, 협력 체제를 구축하였다. 미 연안경비대는 중국의 선전 항과 텐진 항만을 실사한 후 두 항만이 국제협약의 요구에 따라 보안규칙을 시행하고 있고, 많은 인력과 자금을 투입한 것에 대해 높이 평가하였다. 미국은 중국이 비교적 우수한 항만시설 보안시스템을 마련한 것으로 평가하고 있다.

첫째, 모든 신설 부두에 보안요원이 배치되어 있고, 각 항만의 안전 또는 생산 담당자를 포함한 약 5,000명에 달하는 보안요원이 교통부에서 실시한 보안훈련교육에 참가하였다.

둘째, 우범 우려가 있는 인력을 색출하는 데 필요한 전국적인 신분조회와 식별시스템(공안기관의 호적 관리시스템)을 보유하고 있다.

셋째, 선박 적재화물에 대한 통제 강화, 즉 사전에 물품 리스트를 확인하고, 항만에 진입할 때 인원과 차량이 유효한 증명서류를 소지하고 있는지 적절하게 검사하고 있다.

넷째, 항만시설의 연습과 훈련에 있어서 정부기관의 긴밀한 협력 하에 여러 부문이 참가하는 실전 형식을 채택하고 있다.

다섯째, 항만제한구역에 대한 통제가 완벽하다. 항만 내 화물과 항만구역 담장(울타리)간 공간이 크므로, 폐쇄회로(CCTV) 시스템의 감독 및 통제에 유리하다.

여섯째, 항만시설의 경비와 보안상황이 비교적 우수하다.

일곱째, 상하이 보우산(寶山) 컨테이너 터미널은 다른 업무 파트너와 보안계약을 체결하고 있다.

여덟째, Ningbo 공안국의 항만공안지휘센터는 각 보안기관을 지휘 및 조정할 수 있는 시스템을 보유하고 있는데, 지금까지 방문한 기관 중 가장 우수한 통제센터이다.

아홉째, Ningbo 베이룬(北侖) 발전소 터미널은 정기적으로 출입카드 디자인과 색상을 변경하는데, 이는 위조 방지에 있어 하나의 효과적인 방법이다.⁸⁰⁾

(2) 중-미 컨테이너 보안 협정

미국 세관은 2002년 6월에 정식으로 중국의 CSI 가입을 제안하였다. 중국은 같은 해 10월 장쩌민(江澤民) 주석의 미국 방문을 계기로 양국 정상이 원칙적으로 CSI에 가입하여 공동으로 테러행위의 공격을 방지한다는 합의를 이끌어냈다. 그 후 2003년 1월 성광주(盛光祖) 세관당국 부서장을 단장으로 하는 대표단이 미국을 방문하여 미국 세관장에게 CSI를 시행하는 기술적 요건을 제출하였다. 그 후 2003년 7월 29일 양국은 베이징에서 ‘중-미 세관간 CSI협력에 관한 원칙 성명’에 서명함에 따라 두 나라 사이에 컨테이너 화물에 대한 검색사업이 이루어지게 되었다.⁸¹⁾

80) “중국, ISPS 규칙 이행에 있어 세계 선두”, 중국 수운보, 2006. 1. 18.

81) 두 나라 사이의 구체적인 CSI 협정 내용은 다음과 같다. i) 중국은 미국의 CSI 제의를 지지한다. ii) CSI 협력은 양자간 및 국제무역을 최대한 촉진시켜야 한다. iii) 시범으로, 미국은 상하이항과 선전항에 세관원을 파견하고 양국은 공동으로 업무계획을 작성하며, 미국 주재원은 중국의 주권을 존중하고 중국의 법률과 법규를 준수한다. iv) 중국 세관도 대등 원칙에 근거하여 미국 항만에 주재원을 파견한다. v) 합의서 부록에서 미국 주재원의 직책 범위, 업무 절차 등에 대해 구체적으로 규정한다.

2005년 3월 28일 양국은 ‘중국 세관총서와 미국 세관 국경보호국의 CSI협력에 관한 기본 시행절차’를 체결하고 상하이항과 선전항을 시범지역으로 확정하였다. 그 후 2006년 4월 27일 상하이에서 중·미 세관장이 참석한 가운데, CSI 협력 개시식을 개최하였다. 그 외에 테러방지와 관련해 중미 양국은 메가 포트(Mega-port) 프로젝트를 추진하고 있다. 이 사업은 미국 세관 국경보호국과 중국세관총서 및 중국 국가품질 감독검사 검역총국이 2005년 공동으로 체결한 협정을 토대로 하고 있다. 중국과 미국 사이에 CSI 협정 체결을 논의하는 과정에서 부각된 주요 쟁점은 다음과 같다.

① 중국의 주권 침해 문제

미국이 중국에 대해 CSI 가입을 제안하자 중국은 미국 세관에서 파견한 주재원(세관직원)이 검사 컨테이너에 대한 선정과 검사를 수행할 경우 중국의 주권과 사법 독립에 상당한 영향을 미칠 것을 우려하였다. 이에 대해 미국은 위험성이 큰 컨테이너를 발견한 경우 중국 세관이 검사를 수행하고, 미국 주재원은 전체적인 검사과정만 관찰할 것이므로 중국의 주권에 아무런 영향을 미치지 않을 것이라고 강조하였다. 또한 최종적인 검사 여부는 중국세관에서 결정하는 것이라고 설명하였다.

이 같은 내용을 반영하여 합의서 부록 제1조에 “미국은 반드시 중국의 주권을 존중하고, 미국 세관국경보호국에서 컨테이너 보안 검색의 수행목적으로 중국에 파견된 주재원은 반드시 중국의 관련 법률, 법규 및 세관 등 기관의 관련 규정을 엄격히 준수한다는 문구를 삽입하고, 컨테이너 검색은 양국의 협정 범위 내에서 수행되고, 미국 주재원은 어떠한 법 집행 활동에도 참여하지 않는 것으로 입장을 정리하였다. 이에 따라 미국 주재원은 무기를 소지할 수 없고, 화물과 인원에 대한 압류 권한을 가지지 않는다”는 규정을 포함하였다.

② 항만 물류의 효율성 문제

중국은 미국 세관원의 참여로 인해 CSI 협력에 참여하는 항만의 물류 효율

이 떨어지고, 경쟁력이 약화될 우려가 있다고 강조하였다. 실제로 상하이와 선전항의 경우 수출 기업이 세관당국에 화물을 신고하고, 화물이 항만에 도착하여 통관 및 선적까지 모든 과정이 일반적으로 24시간 내에 종료된다. 이 경우 미국의 검사 요구로 시간이 지연된다면 통관 효율은 물론 기업에 대해 추가적인 비용을 발생시킬 가능성도 있다.

이에 대해 미국은 CSI에 참여하게 되면 오히려 컨테이너 화물의 처리가 보다 촉진될 수 있다고 밝혔다. 즉, 일반적으로 화물은 수출에 앞서 부두에서 며칠간 대기하고 있는데, 화물에 대한 검사는 이 같은 대기 기간에 이루어지므로 별도의 추가기간이 발생하지 않으며, 검사를 마친 컨테이너는 미국에 도착하여 빠른 통관을 기대할 수 있기 때문이다.

따라서 양국의 핵심적인 논의는 미국의 검사 요구 시점에 맞춰졌다. 즉, 미국이 어느 시점에서 검사요구를 할 수 있는지, 또한 이와 관련하여 시간제한을 두고 이 기간이 경과한 이후 요구하는 경우 중국은 거부할 수 있는 것으로 입장을 정리하였으며, 그렇지 아니할 경우 이로 인한 책임은 미국이 부담하도록 하였다.

또한 합의서 부록에 “중국이 이미 검사 완료한 화물에 대해 특정한 이유가 없는 한 미국은 일반적으로 재검사를 요구해서는 아니 된다”는 문구를 삽입하였다. 여기서 특정한 이유이라 함은 화물이 항만에서 출발한 후 미국에서 이와 관련된 새로운 위험 정보를 입수한 경우를 의미한다.

③ 정보 시스템의 보안 문제

CSI 협력에 있어서 미국 주재원은 중국세관이 사전에 제공한 컨테이너 선적명세서와 자체 입수한 정보를 분석하여 위험성이 큰 컨테이너를 선별한다. 이로 인해 각각 정보 시스템의 보안 문제를 고려하여 합의서 부록에서 “쌍방은 상대방 세관의 컴퓨터시스템 또는 데이터베이스에 접근할 수 없으며, 쌍방이 필요로 하는 관련 데이터는 합의된 범위와 방식에 따라 제공한다. 그리고 제공된 데이터는 제시한 요구 목적 이외 기타 용도로 이용되지 못 한다”는 문구를

포함하였다.

④ 컨테이너 화물 검색기 설치

비 파괴 컨테이너 화물 검색기 설치에 CSI 협력에 참가하는 하나의 기본요건이다. 중국 세관은 미국의 일부 업체들이 미국 세관과 기타 국가간 CSI 협력 기회를 노려 강제적으로 자신의 표준과 제품을 보급하거나 심지어 덤핑으로 시장점유율을 확대하는 경향을 주시하고 있다.

(3) 중국-유럽연합 세관 협력

2004년에 중국과 유럽연합(EU)은 ‘세관업무에 관한 협력과 행정협조에 관한 협정’을 체결하였다.⁸²⁾ 이 협정은 2005년 4월부터 발효되었다. 이 협정에 따라 중국 세관총서와 EU 세관은 합동으로 세관협력위원회를 설립하고, 공동 관심사에 대한 협력과 의견을 교환하고 있다. 그 후 2006년 중국과 EU는 공급망 전체에서 보안과 무역 원활화에 관한 협력을 강화하기로 합의하였다.

우선 두 진영은 유럽위원회, 중국세관, 영국세관과 네덜란드 세관 등이 참여하는 시범사업을 추진하기로 하였다. 구체적으로는 로테르담 항 및 펠릭스토크항과 중국의 선전 항 사이에 해상 운송 컨테이너에 대한 보안 검사를 강화하기로 결정하였다. 그리고 이 같은 시범사업이 기대한 효과를 거두게 되면 향후 유럽 전체 지역으로 확대할 계획이다.

두 진영이 컨테이너 물류보안에 관한 협력사업을 추진하는 것은 향후 컨테이너 화물의 흐름과 교역 촉진에 상당한 기여를 할 것이라는 점에서 관심을 끌고 있다. 지금까지 미국을 중심으로 민간기업 및 정부 부처가 공동으로 컨테이너 화물 추적사업을 추진한 적은 있으나 정부 간에 양자협정을 토대로 이 같은 사업을 한 사례는 없었기 때문이다. 특히 중국과 유럽연합의 경우 최대 교역 당사국이라는 점에서 이 사업의 성공여부가 향후 물류 흐름에 상당한 영

82) 중국세관 홈페이지(<http://www.customs.gov.cn/YWStaticPage/3292/6f6835d5.htm>)

향을 끼칠 것이 거의 확실하다.

(4) 미국의 C-TPAT 참여

C-TPAT는 미국 국토안전부 세관국경보호국(CBP)이 9·11 테러 이후 제안한 반테러 민관협력 프로그램으로, 2002년 4월 16일부터 정식으로 시행되고 있다. 이 사업을 통해 미국의 CBP는 관련 업계와 협력하여 물류보안 시스템을 구축함으로써 물류 전 구간에서 테러 차단에 주력하고 있다. 이 프로그램에 참여한 회원들은 C-TPAT가 제정한 기준에 따라 자체적으로 관련 시설, 인원, 절차 및 운송 등의 보안 조치를 강화해야 한다.

여기에는 절차보안, 정보처리 보안, 접근 통제 및 감독, 인원보안, 보안 교육 훈련, 선적 명세서 신청절차와 운송보안 등 8개 내용이 포함된다. 그 외에 C-TPAT 회원은 파트너 또는 협력업체에게 공동으로 공급망의 보안을 확고히 할 것을 요구할 수 있다. 현재 중국의 COSCO 등 대형 선사들이 미국 파트너의 요구에 따라 C-TPAT에 참여하고 있다.

5) 시사점

중국의 현재 물류보안에 관한 국제규범을 시행하는 한편, 미국 등과는 양자 협정을 맺어 필요한 보안조치를 마련하고 있다. 전자의 대표적인 사례로 IMO의 ISPS 코드를 수용해 선박과 항만시설의 보안을 확보하는 한 것을 들 수 있다. 또한 미국과는 CSI 협정을, 그리고 유럽연합과는 세관협정을 체결해 컨테이너 화물의 국제간 이동을 촉진하는 한편, 물류보안도 강화하고 있다.

그런데 중국이 이 같은 물류보안조치를 시행하면서, 특히 미국과의 CSI 협정을 체결하면서 자국에서 일어날 수 있는 모든 문제점에 대한 제어장치를 마련하였다는 점을 높이 평가할 수 있다. CSI 협정서 부속서에 미국 세관 주재원에 대해 중국의 법률에 따라 업무를 처리하도록 한 점, 총기 휴대 금지 및 컨테이너 화물 운송과 관련된 사람이나 화물 자체에 대해 압류권을 행사하지

못하도록 못 박은 것이 특히 그러하다. 이 같은 문구를 넣은 것에 그치지 않고, 중국은 아직까지 안보상의 이유를 들어 미국 세관원의 자국 주재를 허용하지 않고 있다.

이 뿐만 아니라 중국은 컨테이너 화물 정보가 미국에 제공되어 악용되는 소지를 방지하기 위해 화물 검사 목적 이외에는 절대 사용할 수 없도록 하는 문구를 포함하였다. CSI 협정을 체결하면서 미국에 화물을 수출하는 중국 화주, 제조업체들의 우려를 반영한 조치로 풀이되고 있다. 미국과의 CSI 협정문서에 이 같은 문구를 삽입한 것은 중국이 거의 유일한 사례로 알려지고 있다.

한편, 중국은 컨테이너 화물 검색기에 대해서도 자국의 기술 개발과 판매를 적극 지원하는 정책을 추진하는 것으로 보인다. CSI를 체결하면서 미국의 자국 업체의 제품을 표준으로 선정하는 것에 대해 제동을 거는 한편, 자체적인 연구·개발(R&D) 사업으로 상용화된 시스템을 적극 활용하고 있다. 우리나라 세관 당국이 도입해 사용하고 있는 Nuctech 사의 컨테이너 화물 검색기가 그것이다. 즉, 중국은 국제적으로 강화되고 있는 물류보안제도를 수용하는 한편, 이를 비즈니스 모델로 활용하는 양면 전략을 구사하고 있다.

제5장

우리나라 물류보안제도 시행 현황

1. 보안관련 법률과 각 부처의 업무

1) 국방부

(1) 통합방위법과 통합방위대책 수립

국방부는 통합방위⁸³⁾법에 의해 적의 침투·도발이나 그 위협에 있어서 국가 총력전의 개념에 입각하여 국가방위요소를 통합·운용하기 위한 통합방위 대책을 수립·시행하고 있다(동 법 제1조). 이를 위해 정부에게 국가방위요소의 육성 및 통합방위태세의 확립을 위하여 필요한 시책을 강구하도록 요구하고(제3조 제1항), 각 중앙관서의 장에게 구체적인 업무를 부과하고 있다(시행령 제2조 제1항). 통합방위법에 의하면 기본적으로 국가중요시설의 경비·보안 및 방호 책임은 그 시설의 소유자나 관리자 (이하 “소유주”라 한다)에게 있다. 따라서 시설주에게 국가중요시설의 경비·보안 및 방호를 위해 부여된 업무는 다음과 같다(동법 시행령 제23조의 2).

- i) 청원경찰, 특수경비원, 직장예비군 및 직장민방위대 등 방호인력, 장애물 및 과학적인 감시 장비를 통합하는 것을 내용으로 하는 자체방호계획의 수립·시행
- ii) 국가중요시설의 자체방호를 위한 통합 상황실과 지휘·통신망의 구성

83) 여기서 통합방위라 함은 적의 침투·도발이나 그 위협에 있어서 각종 국가방위요소를 통합하고 지휘체계를 일원화하여 국가를 방위하는 것을 말함.

등 필요한 대비책 강구

iii) 자체방호계획에는 시설주 및 특수경비업자의 책임 하에 실시하는 통합 방위법령과 시설의 경비·보안 및 방호업무에 관한 직무교육과 개인화기를 사용하는 실제의 사격훈련에 관한 사항 포함

한편 지방경찰청장 및 지역군 사령관에게는 군·경찰·향토예비군 및 민방 위대 등의 국가방위요소를 통합하는 것을 내용으로 하는 관할지역 안의 국가 중요시설에 대한 방호지원계획 수립·시행의무를 부과하고 있다.

또한 합동참모본부에는 통합방위본부를 두고 있으며, 통합방위본부는 i) 통합방위정책의 수립·조정, ii) 통합방위 대비태세의 확인·감독, iii) 통합방위 작전상황의 종합분석 및 대비책의 수립, iv) 통합방위작전·훈련지침 및 계획의 수립과 그 시행의 조정·통제, v) 통합방위 관계기관간의 업무협조 및 사업집행사항의 협의·조정 등의 업무를 수행한다.

(2) 통합방위지침과 국가중요시설 보호

국방부는 적의 침투·도발이나 그 위협에 대비하여 국가중요시설에 대해 통합방위대책을 수립하고 있다. 국가중요시설은 실질적으로 국가정보원장이 분류하고 있는데, 국가중요시설의 분류는 <표 5-1>과 같다.

〈표 5-1〉 국가중요시설의 분류

구분	분류	항만
가 급	국가의 안전보장에 고도의 영향을 끼치는 행정·산업시설, 청와대, 국회의사당, 대법원, 정부종합청사, 국방부, 국가정보원, 한국은행본점	1만톤 이상의 선박출입이 가능하고, 동시접안능력 100만톤 이상
나 급	국가보안상 국가경제 또는 사회생활에 중대한 영향을 끼치는 행정·산업시설, 경찰청, 대검찰청, 국책은행 및 시중은행본점	1만톤 이상의 선박출입이 가능하고, 동시접안능력 50만톤 이상
다 급	국가보안상 국가경제 또는 사회생활에 중요하다고 인정되는 행정·산업시설, 기타 중앙행정기관이 정하는 시설	동시접안능력 10만톤 이상, 여객운송 및 주요생활필수품 취급도서에 위치한 항만, 특별한 보호가 요구되는 항만
기타 급	중앙부처장 또는 시·도지사가 필요하다고 지정한 행정·산업시설로서 중요도는 별로 없는 시설	

항만, 선박교통로, 공항 등의 국가중요시설이며, 동시에 중요물류시설이다. 통합방위지침은 중앙행정기관의 장에게 소관 국가중요시설에 대하여 시설주로서 경비·보안 및 방호대책 수립·시행의무를 부과하고 있다(동 지침 제4조). 동시에 중앙행정기관 장은 소관 국가중요시설(특별법, 직제령, 기타 규정에 의해 편성 운영되는 예하기관)의 시설주의 자체방호계획 수립의 적절성, 취약점 유무를 지도 감독할 의무가 있다(통합방위지침 세부시행지침 제24조). 그러므로 국방부의 물류보안과 관련한 역할은 중요물류시설의 방호에 관한 총괄책임이다.

2) 국가정보원

(1) 통합방위법과 물류시설 보안 책임

통합방위법은 국가중요시설의 시설주에게 경비·보안책임과 통합방위사태에 대비하여 자체방호계획을 수립의무를 부여하고, 통합방위사태에 대비한 국가중요시설의 방호에 관한 총괄책임은 국방부에 부여하고 있다. 그러나 국가중요시설의 평시 경비·보안활동에 대한 지도·감독권한은 관계행정기관의 장과 국가정보원장에게 부과하고 있다(제15조의 2).

(2) 보안업무규정과 국가보안목표시설 보안책임

국가정보원의 주요직무 중의 하나가 국가기밀에 속하는 문서·자재·시설 및 지역에 대한 보안업무이다(국가정보원법 제3조 제2호).

국정원장은 국가보안에 관련된 시설·자재 또는 지역을 파괴·태업 또는 비밀누설로부터 보호하기 위하여 보안측정을 실시한다(제35조). 보안측정은 파괴·태업 또는 비밀누설로 인하여 전략적 또는 군사적으로 막대한 손해를 초래하거나 국가안전보장에 연쇄적 혼란을 초래할 우려가 있는 시설 또는 지역(이하 “보안목표시설”이라 한다)과 선박·항공기 등 중요장비(이하 “보호장비”라 한다)에 대하여 실시한다(제36조). ‘대형선박의 출입항이 가능한 항만’은 보

안측정대상이다(보안업무규정 시행규칙 59조).

(3) 국가보안목표관리지침과 국가보안목표시설 보안책임

통합방위법과 마찬가지로 국가보안목표관리지침도 시설주에게 국가보안 목표시설의 보호를 위한 자체 경비·보안계획을 수립·시행 및 경비상황실 설치·운용의무를 부여하고 있다(제6조 및 제7조). 시설주가 경비·보안계획을 수립할 때에는 감독기관의 협의·조정을 받아야 한다(제6조 제5항). 운송업자는 계류(정박중인 항공기(선박)에 대한 불법 침입, 폭발물 탑재 등 위해행위 방지를 위해 기내 출입자 및 반출입 물품에 대한 확인 등 통제와 경비를 실시하고, 운항중인 선박의 보안관리 대책 강구하여야 한다(제14조 및 제15조).

3) 해양수산부

(1) 보안관련 상위 법률과 선박 및 항만의 보안

① 통합방위지침

통합방위법 시행령 규정에 따라 통합방위지침은 해양수산부 장관에게 항만 및 해상교통로 등의 국가중요시설에 대한 경비·보안 및 방호대책 수립·시행 의무를 부과하고 있다(제4조 13호 바).

② 국가중요시설 경비, 보안 및 방호업무에 대한 시행지침

중앙행정기관 장(해양수산부)은 소관 국가중요시설(특별법, 직제령, 기타 규정에 의해 편성 운영되는 예하기관)의 시설주의 자체방호계획 수립의 적절성, 취약점 유무를 지도·감독해야 한다(동 지침 법제8조 및 제15조의 2, 시행령 11조).

③ 보안업무규정

보안업무규정 제36조(측정대상) 및 동 규정 시행규칙 제59조(보안측정 대상) 의거하여 ‘대형선박의 출입항이 가능한 항만’은 보안측정대상이다(제3조 제7호). 시설주는 국가보안목표시설의 보호를 위해 자체 경비·보안계획을 수립 시행하고, 경비상황실을 설치·운영하여야 한다(제6조 및 제7조).

운송업자는 계류(정박중인 항공기(선박)에 대한 불법 침입, 폭발물 탑재 등 위해행위 방지를 위해 기내 출입자 및 반출입 물품에 대한 확인 등 통제와 경비를 실시하고, 운항중인 선박의 보안관리 대책 강구(제14조 및 제15조). 항만에 정박하고 있는 선박의 경비·보안에 관한 사항은 항만시설주의 지도·조정을 받는다(제14조 제3항). 시설주와 감독기관(해양수산부 소속 기관장)으로 구성된 항만 보안대책협의회 구성·운영하여야 한다(제23조).

(2) 항만법과 항만시설 보안책임

항만법에는 항만시설의 관리와 화물의 경비 등에 관한 일반적인 규정을 두고 있을 뿐 IMO 협약에서 요구하고 있는 항만시설의 보안 등에 관한 규정은 없다. 즉, 해양수산부 장관은 항만시설의 관리와 화물의 경비 등을 위하여 필요한 경우에는 항만의 관리를 위한 법인을 둘 수 있다(항만법 제70조 및 시행령 제40조). 부산항부두관리공사 등 항만관리법인은 매 사업연도의 사업계획 및 예산·결산에 대하여 해양수산부 장관을 승인 받아야 하고, 그 업무 및 회계에 관하여 지도·감독을 받는다(시행령 제41조).

(3) 항만공사법과 항만시설 보안책임

항만공사법은 항만시설의 경비·보안 및 항만안전에 관한 사항에 대해 해양수산부 장관이 항만공사를 지도·감독할 수 있게 하고 있다(법 제37조 및 시행령 제29조).

2. 해운·항만 부문 보안 제도

1) 관련 규정

(1) 항만경비 및 보안관리지침

① 목적

보안업무규정과 통합방위지침(대통령훈령 제28호)의 규정에 의하여 국가보안목표시설로 지정된 항만보호구역의 경비 및 보안관리에 필요한 사항을 규정한 것이다.

② 경비·보안책임

지방해양수산청장이 관할항만 전체에 대하여 경비·보안책임을 지되 항만보호구역에서의 민유 시설주 및 항만시설 임대계약자가 전용 사용하는 시설에 대하여는 그 책임 하에 경비·보안업무를 수행하여야 한다(제3조 제1항).

지방해양수산청장은 당해 항만보호구역의 경비·보안업무를 수행함에 있어 경비·보안에 관한 지휘감독권을 일원화하여야 하며, 당해 항만의 경비본부장이 된다(제3조 제3항). 지방해양수산청장은 항만법에 의해 설립된 항만관리법인에게 경비·보안관리 업무와 그 지휘감독권을 위탁할 수 있으나 항만경비·보안 상황을 파악·통제하여야 한다(제3조 제4항). 항만관리법인은 지방해양수산청장으로부터 항만보호구역의 경비·보안관리 업무와 그 지휘권을 위탁받은 범위 내에서 책임을 진다(제3조 제1항 2호). 지방청장은 항만보호구역에 대한 테러 및 안보위해상황 등 우발사태에 대처할 수 있도록 항만종합상황실을 설치하고, 유관기관과 유기적인 협조체제를 구축하여야 한다(제4조 제1항).

(2) 선박 및 항만시설의 보안에 관한 규정

① 제정사유

미국의 9·11 항공기 테러 이후 해상과 항만에서의 보안강화를 위해 IMO (국제해사기구)에서 2002. 12. 12 채택한 ISPS Code(국제선박및항만시설보안규칙)가 2004. 7. 1일 이후 국제적으로 시행되고 있다. 우리나라는 ISPS Code 발효시기의 시급성으로 2003년 10월에 「선박및항만시설보안에관한규정(고시)」을 우선 제정, 시행하고 있다.

② 규정 주요내용

- 적용대상 : 국제항해 취항 여객선 · 총톤수 500톤 이상 화물선 · 이동식 해상구조물 및 국제항해 선박들이 이용하는 항만시설로 하였다(제3조).
- 보안관리체제 점검 : 지방해양수산청장으로 하여금 관할 항만내 정박 중이거나 입항하고자 하는 외국선박에 대하여 보안관리체제가 국제기준에 적합한지 여부를 점검하도록 하고 있다(제7조).
- 보안등급 : 선박 및 항만시설의 보안등급은 보안수준에 따라 3단계로 구분하여 설정 · 조정할 수 있도록 하고 있다(제10조, 제11조).
- 보안위원회 설치 · 운영 : 선박 및 항만시설의 보안관리 업무를 효율적으로 처리하기 위하여 심의 · 자문기관으로 외부전문가를 참여시킬 수 있는 보안위원회를 설치 · 운영할 수 있도록 하였다(제12조).
- 보안책임자 : 선박회사는 회사보안책임자 및 선박보안책임자를 임명하고, 소속 선박에 대한 보안평가를 실시 후 보안계획서를 작성하여 지방해양수산청장의 승인을 받도록 하였다(제15조, 제16조).
- 선박이력기록부 비치 : 선박회사는 지방해양수산청장으로부터 선박이력기록부를 교부받아 이를 선내에 비치하도록 하고 있다(제21조).
- 선박보안경보장치 탑재 : 선박은 선종에 따라 단계적으로 선박보안경보

장치를 탑재하도록 하였다. 여객선, 500톤 이상 위험물운반선 : 2004. 7. 1 이후 도래하는 첫 번째 무선검사일, 그리고 500톤 이상 기타화물선 : 2006. 7. 1 이후 도래하는 첫 번째 무선 검사일까지 탑재토록 하였다(제22조).

- 선박식별번호 표시 : 선박은 2004년 7월 1일 이후 계획된 최초 입거 검사일까지 선박식별번호를 영구 표시하여야 한다(제23조).
- 보안계획서 작성 : 지방해양수산청장은 관할 각 항만시설에 대하여 보안책임자를 임명하고, 항만시설 보안평가를 시행하여 항만시설보안계획서를 작성한 후 해양수산부 장관의 승인을 받아야 한다(제25조 내지 제28조).
- 교육훈련 : 선박회사 및 지방해양수산청장은 소속 회사와 선박 및 항만시설의 보안책임자와 보안업무 담당자에 대하여 교육·훈련계획을 수립하여 시행하여야 한다(제29조 내지 제31조).
- 보안교육기관 지정 : 보안교육을 실시하고자 하는 기관은 해양수산부 장관으로부터 보안교육기관으로 지정을 받아야 한다(제32조).
- 국제선박보안증서 비치 : 보안심사회사는 소속 선박에 대하여 지방해양수산청장으로부터 보안심사를 받아 국제선박보안증서(유효기간 5년)를 선내에 비치하여야 한다(제33조 내지 제45조).
- 보안심사업무 대행 : 해양수산부 장관은 불가피한 경우 선박의 보안심사에 관한 업무를 외부 전문기관에 대행하게 할 수 있도록 한다(46조 내지 제50조).

2) 항만경비보안 주체 및 운영방식

(1) 부산항

부산항의 경비보안업무는 항만법에 의해 설립된 항만관리법인인 부산항부두관리공사가 수행하고 있다. 부산 항만경비 및 보안업무 운영체척상 부산항만의

경비·보안업무의 책임분장은 다음과 같다(제7조).

〈표 5-2〉 부산항 경비·보안업무 책임 분장

구분	책임 분장
부산지방해양수산청장	부산항의 경비·보안에 관하여 총괄책임
부산항만공사 사장	부산항의 소유주와 관리주로서의 경비·보안에 대한 책임
부산항부두관리공사 사장	부산항만공사 사장으로부터 위탁받은 사항에 대하여 책임

자료 : 한국해양수산개발원

그리고 부산항 경비 및 보안업무 운영세칙에서 규정하고 있는 각 경비주체별 구체적인 업무는 다음과 같다.

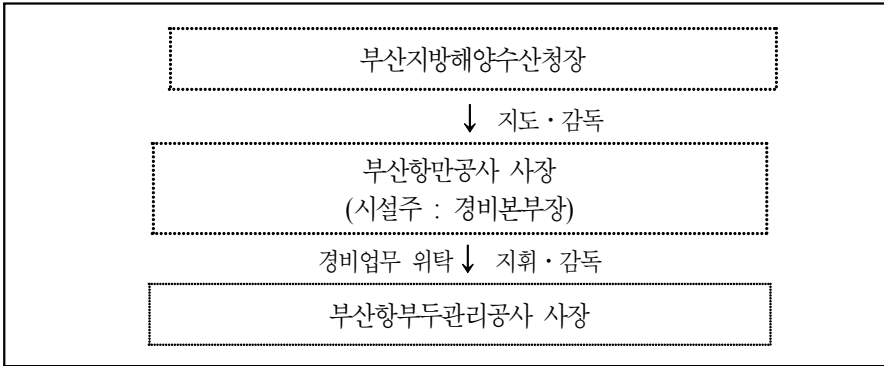
i) 부산지방 해양수산청 : 부산항의 경비·보안업무의 총괄, 부산항만의 경비·보안장비 및 보안시설의 운영관리 실태점검 및그 에 따른 조치와 항만안전에 관하여 부산항만공사의 경비·보안업무 지도감독(제3조), ‘부산항만종합상황실 설치·운영(제6조)

ii) 부산항만공사 : 부산항의 소유주 및 관리주로서의 경비·보안계획의 수립·시행에 관한 업무, 경비·보안업무의 부산항부두관리공사 위탁, 부산항부두관리공사의 임원·사업계획·예산 승인, 항만 출입증 발급 등 항만출입관리업무 수행(제4조)

iii) 부산항부두관리공사 : 부산항만공사로부터 위탁받은 부산항 항만시설의 경비·보안업무 범위 내에서 경비·보안업무 집행, 즉 항만경비보안·대테러대책·특별경계근무 강화 세부계획 수립·보고 및 시행, 항만순찰 및 경비종합 계획 수립·시행(제5조)

그리고 부산항만 경비보안에 대한 지휘체계는 <그림 5-1>과 같다. 이러한 체제는 항만공사가 운영되는 인천도 유사하다.

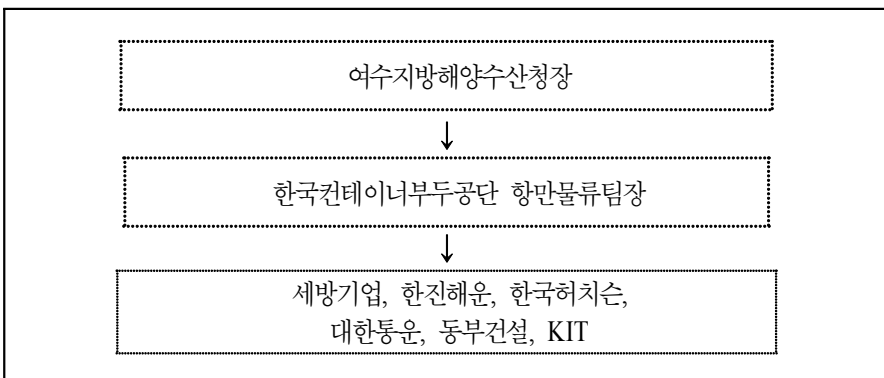
〈그림 5-1〉 부산항만 경비보안 지휘체계



(2) 여수(광양)항

여수(광양)항의 “항만경비및보안관리규정”에 의하면 여수(광양)항 경비보안 책임자는 여수지방해양수산청장이다. 여수항 및 광양항 공용부두는 여수지방 해양수산청이 청원경찰을 고용하여 경비하며, 광양항의 포철부두 등 임대부두와 컨테이너부두는 임차인이 경비보안 책임을 진다. 광양항 컨테이너부두는 2004년 2월부터는 한국컨테이너부두공단과 광양항 컨테이너 터미널운영사 간에 체결한 ‘경비업무에 관한 협약’에 따르고 있다. 광양항 컨테이너부두의 지휘·감독 체계는 <그림 5-2>와 같다.

〈그림 5-2〉 광양항 컨테이너부두의 지휘·감독 체계



3) ISPS Code의 발효와 국내 대응조치

(1) 선박보안과 관련한 대응 조치

① 사전대응 조치

우리나라는 ISPS Code의 국내수용 기반을 조성하기 위하여 국내시행규정을 신속히 제정하고 선박의 보안평가서·보안계획서 모델 개발 및 보안관련 교육을 통하여 전문인력을 양성하였다. 선박보안관련 사전 대응조치 및 주요내용은 <표 5-3>과 같다.

<표 5-3> ISPS Code 시행을 위한 사전 대응조치

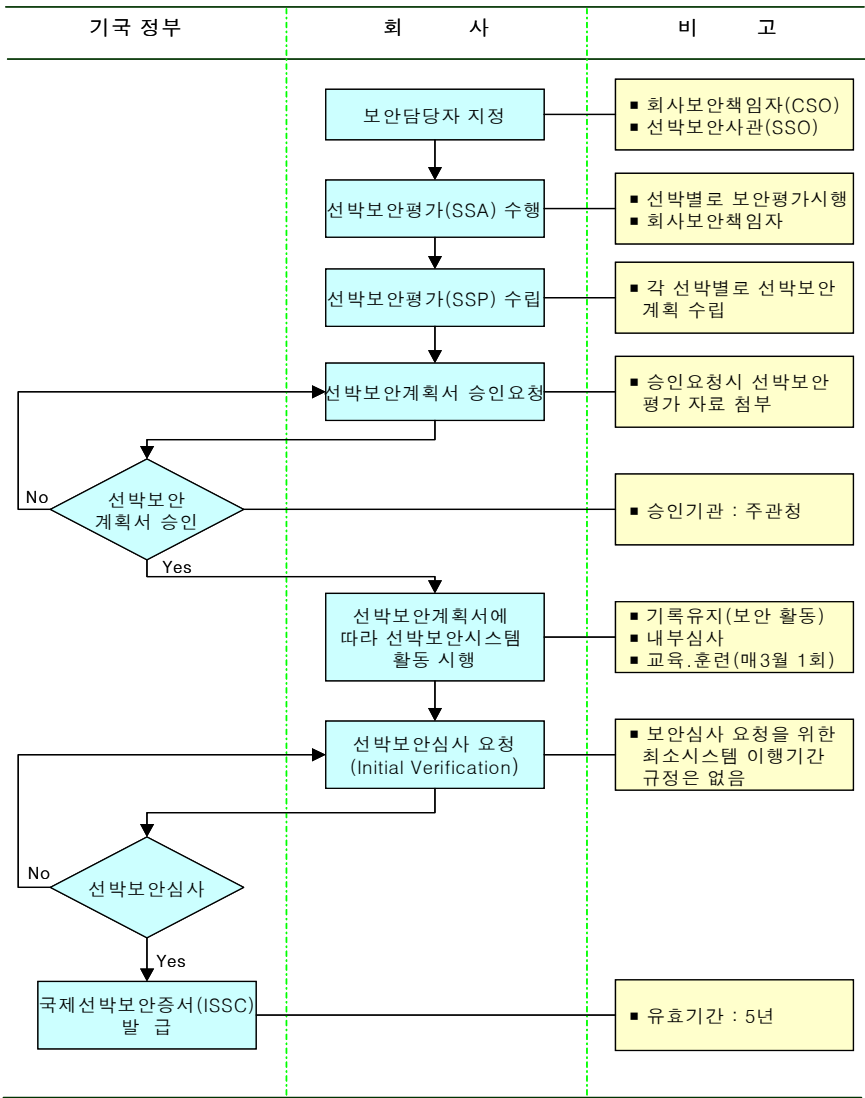
대응조치	내용
전문가 및 관련업계 실무자 Working group 운영('03.3~'03.10)	보안평가서·보안계획서 모델 개발 및 보안교육 방안 등 검토
국내수용을 위한 국내규정 제정 추진('03.7~'03.10)	선박및항만시설보안에관한규정' 제정(해양수산부고시('03.10.25))
선박보안심사원 양성교육 실시('03.10~'04.2)	지방청 항만국통제(PSC) 인력(65명)에 대하여 선박보안계획서 승인과 보안심사를 위한 교육 및 선박보안평가 현장 교육 실시
보안책임자 교육을 위한 보안교육기관 지정('03.11.4)	한국해양수산연수원, 한국선급
선박보안계획서 승인업무 개시('03.11.7, 부산청)	선박보안계획서 승인 완료(425척, '04.5.29)
선박보안심사 및 국제선박보안증서 발급 개시('04.1.15, 포항청)	선박보안계획 이행 여부 등 심사 및 국제선박보안증서(5년) 발급

자료 : 해양수산부 홈페이지

국제항해선박은 보안계획을 수립하여 승인을 받은 후 보안이행에 대한 심사를 받고 선박보안증서(유효기간 5년)를 교부받아 비치·운항하여야 한다. 선박보안계획서에는 선박보안담당자 지정 및 임무 부여, 선박출입자 출입통제 요령, 선박보안경보장치 작동 요령, 보안교육·훈련 방법 등이 포함되어야 한다. 선박보안 인증절차는 <그림 5-3>과 같다.

우리나라는 ISPS Code가 시행되기 된 2004년 7월 1일 전에 96개의 회사와 425척의 국적선이 선박보안 인증을 완료하였다.

〈그림 5-3〉 선박보안 인증절차



자료 : 해양수산부, ISPS Code의 국내수용방안 연구, p. 28.

② 선박보안 책임기관 등 지정 및 종합상황실 운영

우리나라의 선박보안 책임담당기관은 해양수산부 안전정책과로 지정되어 있으며, 선박과 육상 간의 보안정보의 접수 및 조치기관으로는 해양수산부와 해양경찰청이 지정되어 있고, 담당부서는 해양수산부 종합상황실이다. 또한 타 당사국으로부터 국제선박에 대한 해상보안관련 통신접수 담당부서도 종합상황실이다. 이러한 업무를 수행할 수 있도록 선박에서 테러 등 침입을 알리는 보안경보신호를 수신할 수 있는 선박보안감시시스템을 해양수산부 종합상황실에 구축하였다. 이 시스템을 통하여 수신된 경보신호는 해양경찰청 및 연안국 정부에 실시간 전파하여 대응토록 조치하고 있다. 우리나라 관할 영역내에서 국제선박 및 외국적 선박으로부터 보안정보가 접수될 경우 선박지원업무는 해양수산부 종합상황실의 지시에 따라 해양경찰청 종합상황실을 경유하여 관한 지방해양경찰서에서 수행하고 있다.

③ 항만국 통제 실시

보안이 취약한 외국선박으로부터 우리항만을 보호하기 위하여 국내항에 입항하고자 하는 외국선박에 대하여 보안점검을 실시하고 있다. 점검사항은 선박 보안증서 비치, 보안계획 이행여부 등의 확인이다.

④ 선박 및 회사의 조치

ISPS Code에 따라 선박 및 회사가 선박보안을 위하여 취하여야 할 조치는 다음과 같다. 회사 및 선박이 취하여야 할 최우선 조치는 국제선박보안증서의 발급 및 비치이다. 2004년 7월 1일 ISPS Code 발효 후에도 국제선박보안증서의 발급은 계속되어 2005년 12월말 기준으로는 125개 회사, 548척이 국제선박보안증서를 발급받아 비치하고 있다.

- i) 회사보안책임자(CSO) 및 선박보안책임자(SSO)의 지정
- ii) 회사보안책임자에 의한 선박보안 평가 수행
- iii) 선박보안계획서(SSP)의 승인 및 비치, 접근통제, 선박보안시스템(SSAS)

설치

- iv) 보안활동 기록유지 및 관계자 교육·훈련 실시
- v) 국제선박보안증서 및 선박이력기록부 비치
- vi) 입항전 선박 보안정보(SSI) 항만당국에 통보

(2) 항만시설 보안관련 대응조치

① 협약 발효 전 대응조치

국제항만시설의 보안과 관련하여 협약 발효전 사전대응조치 사항은 <표 5-4>와 같다.

〈표 5-4〉 협약시행을 위한 사전 추진현황

대응조치	내용
전문가 및 관련업계 실무자 Working group 운영 ('03.3~'03.10)	보안평가서·보안계획서 모델 개발 및 보안교육 방안 등 검토
항만보안 자문기관을 지정하여 ISPS Code 보다 강화된 지침 마련('04.4~)	- 한국선급을 자문기관으로 지정 - 미국지침, IMO/ILO 코드, ISO표준안을 종합한 국내지침 마련 및 미국의 보안평가 체크리스트, 보안계획서 수립절차등을 반영
항만보안 담당자 교육 실시('03.11~'04.5)	지방청 및 민간운영부두 항만시설보안책임자(4회/약 400명)에 대하여 보안평가절차, 보안계획서 작성방법 등에 대한 교육실시
보안적합확인서 발급 및 IMO 등록완료('04.6.25)	28개 항만 123개 시설

자료 : 해양수산부

② 조직

항만보안관련 ISPS Code 이행 주관기관은 해양수산부(해운물류국)이며, 지정당국(Designated Authority)인 지방해양수산청에서 항만시설에 대한 현장관

리 및 감독 업무를 수행하고 있다. 지정당국은 항만시설보안책임자(PFSO)를 지정하여야 하는데, 전용 및 민유 터미널마다 각각 항만시설 보안책임자를 지정하고 있다. 한편, ISPS Code에 대한 범정부적인 대응체제를 구축을 위해 관계부처 관계관으로 구성된 항만보안위원회를 구성하였다. 항만보안위원회는 해양수산부 해운물류국장·안전관리관(위원장), 국정원, 관세청, 해양경찰청 관련 과장 등 14명으로 구성되어 있다.

③ 보안계획서 승인 및 적합확인서 발급

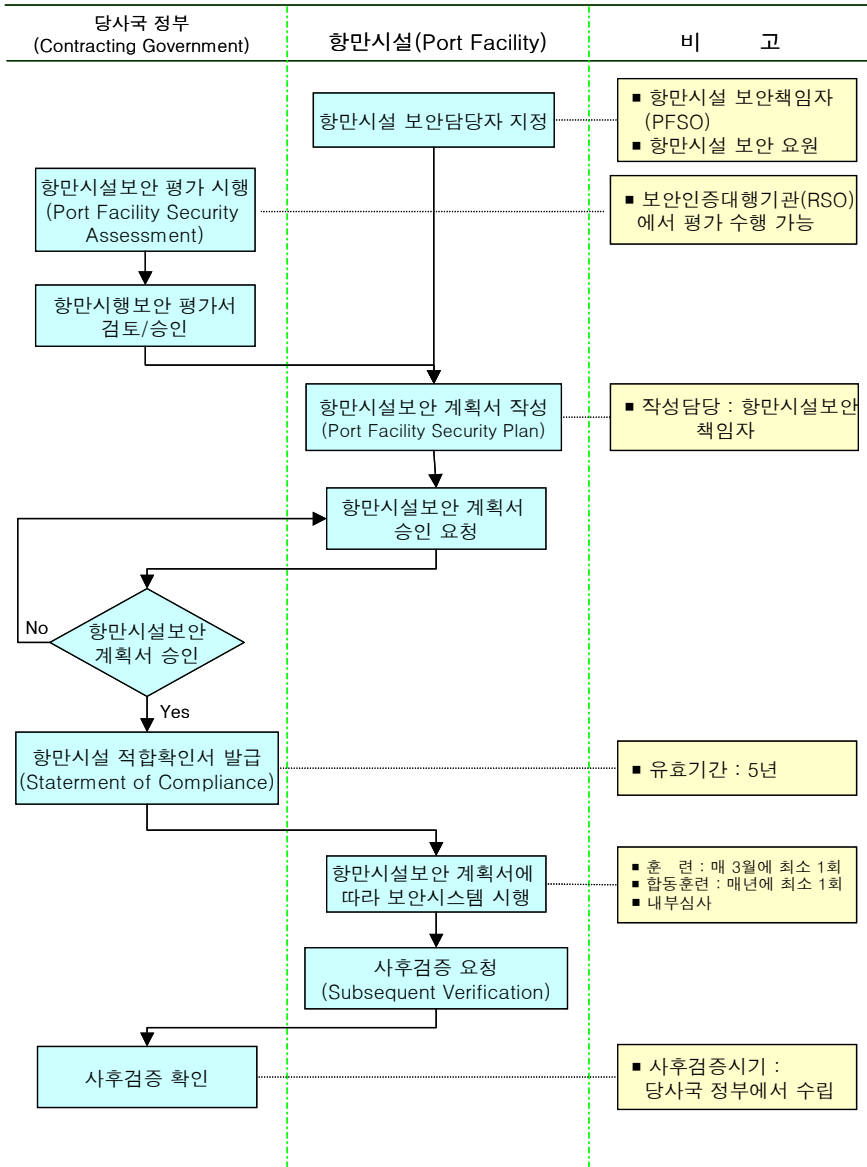
항만별로 국정원 등 보안전문기관과 합동으로 현장자문 및 점검(2회)을 거쳐 「보안평가」를 실시하였다. 또한 국정원, 해경 등으로 항만별로 구성되어 있는 항만보안대책협의회의 심의를 거쳐 「보안계획서」를 수립·승인하고, 「적합확인서」의 발급하였다.

④ 항만시설에 대한 보안조치

ISPS Code에 의한 항만시설의 범위는 우리나라 항만법상의 규정과 다르다. 선박과 항만의 인터페이스(상호작용)⁸⁴⁾가 발생하는 당사국 정부 또는 지정당국에 의해 결정된 장소를 말한다. 따라서 묘박지, 대기선석, 진입수역도 항만시설의 범위에 포함된다. 항만시설보안책임자는 항만시설 보안평가(PFSA)를 시행한 후 작성하여 승인받은 항만시설보안계획서(PFSP)에 따라 보안시스템 활동을 한다(<그림 5-4> 참조). 외국선박이 우리나라 항만에 입항하고자 하는 경우에는 24시간 전에 지방해양수산청 항만통제 전담부서에서 선박보안정보(SSI)를 받아 처리하고 있다. 통보받는 사항은 선박보안등급, 선박제원, 적하물, 승무원 명부, 이전 10회 기항지 등이다. 선박보안정보 접수 후 당해선박의 입항으로 항만시설에 위협이 예상되는 경우에는 입항거부, 추방 등의 조치를 취하고 있다.

84) “선박과 항만의 인터페이스(Ship/port interface)”는 인원, 화물의이동 또는 선박에 대하여 또는 선박으로부터의 항만서비스의 제공을 포함한 활동이 선박에 직·간접적으로 영향을 미칠 때 야기되는 상호작용을 말한다(SOLAS협약 제XI-2장 제1규칙 제8항).

〈그림 5-4〉 항만보안 인증절차



자료 : 해양수산부, ISPS Code의 국내수용방안 연구, p. 29.

(3) 협약이행을 위한 국내 법률정비

① ISPS Code 이행법률

가. 국제 선박 및 항만시설 보안에 관한 규정

2003년 10월 25일에 ISPS Code의 국내 수용을 위하여 “국제 선박 및 항만 시설 보안에 관한 규정(해양수산부 고시 제2003-65호)”를 제정하여 시행하고 있다. 그러나 이 규정은 ISPS협약의 발효시기인 2004년 7월 1일에 맞추어 관련 준비가 완료되어야 하므로 사전 준비기간(약 1년) 등을 고려하여 고시로 우선 제정·시행한 후 법률화를 추진하기로 한 것이다.⁸⁵⁾

나. 선박 및 항만시설 보안에 관한 법률 제정안

ISPS Code 이행을 위해 고시로는 실효성 확보가 곤란함으로 국제협약 시행에 만전을 기하고, 선박과 항만시설에 대한 보안위협을 예방하여 국민의 생명과 재산을 보호하기 위하여 미비된 사항을 보완한 법률 제정을 추진하고 있다.⁸⁶⁾ 2006년 7월 현재 법제처 심의 중인 「선박 및 항만시설 보안에 관한 법률 제정안」의 주요내용은 다음과 같다.

가) 적용범위

국제항해에 사용되는 모든 여객선, 총톤수 500톤 이상 화물선 및 국제항해 선박이 이용하는 항만시설로 규정하고 있다(안 제3조).

나) 보안계획

항만시설보안에 관한 기본방침과 중·장기 추진방향 등을 정하기 위하여 해양수산부 장관에게 국가항만보안계획을 10년 단위로 수립·시행하도록 하고,

85) 「선박 및 항만시설 보안에 관한 규정(고시)」의 규제심사에 대해 ‘06까지 법제화 조건으로 원안동의(제178차 경제2분과위원회).

86) 2006년 6월말 현재 규제개혁위원회 심사중임.

지방해양수산청장은 국가항만보안계획에 따라 지역항만보안계획을 수립하도록 규정하고 있다(안 제5조).

다) 보안위원회 구성·운영

국가항만보안계획의 수립과 보안등급의 설정 등에 관한 사항을 심의하는 보안위원회를 해양수산부 장관 소속하에 두도록 하고 보안위원회 구성·운영 등에 관한 사항은 하위법령에 위임(안 제6조)

라) 선박 및 항만시설에 대한 보안등급의 설정·조정

선박 및 항만시설에 대한 보안등급의 설정·조정 등 근거규정 마련하고, 보안등급의 구분·보안등급별 보안활동 사항 등은 하위법령에 위임(안 제7조) 근거규정 마련하고 보안등급의 구분·보안등급별 보안활동 사항 등은 하위법령에 위임(안 제7조)

마) 항만국 통제 근거

대한민국 항만에 있거나 입항하고자 하는 외국선박에 대하여 당해 선박의 보안관리체제가 국제협약의 기준에 적합한지 여부를 점검할 수 있는 항만국 통제의 근거규정 마련하여야 한다.(안 제10조)

바) 선박보안확보

대한민국 선박의 보안확보에 필요한 회사보안책임자·선박보안책임자 지정, 선박보안평가 실시, 선박보안계획서 작성·승인, 선박이력기록부 비치, 선박보안경보장치 등 설치 및 선박식별번호 표시 등의 근거규정을 마련하였다(안 제12조 내지 제20조).

사) 항만시설 보안확보

항만시설 보안확보에 필요한 항만시설주의 보안책임과 의무, 항만경비·검색 인력 및 보안시설의 확보, 항만시설 보안료, 항만시설보안책임자 지정, 항만시설보안평가 실시 및 항만시설보안계획서 작성·승인, 항만시설 이용자의 보

안유지 의무 등의 근거규정 마련하였다(안 제21조 내지 제29조).

아) 선박·항만시설에 대한 보안심사

선박·항만시설에 대한 보안심사 및 보안증서 교부, 보안심사업무의 대행 및 선박·항만시설에 대한 해양수산부 장관의 지도·감독 등의 근거규정을 마련하였다(안 제30조 내지 제36조).

자) 보안교육 및 훈련실시

선박회사 및 항만시설주의 소속 보안책임자·보안담당자 등에 대한 보안교육 및 훈련 실시 근거규정과 해양수산부 장관의 보안교육기관 지정 근거규정을 마련하였다(안 제37조 내지 제39조).

차) 과태료 부가 근거

국제협약 시행에 만전을 기하고, 선박과 항만시설에 대한 보안위협을 예방하여 국민의 생명과 재산을 보호하기 위한 선박소유자 및 항만시설주의 성실한 보안체제 수립·이행과, 규정의 이행 강제력 및 준법성을 확보하기 위하여 과태료 부과 관련 근거규정을 마련하였다(안 제48조).

② 1998년 SUA협약과 국내 법률정비

가. 제정이유

「선박 및 해상구조물에 대한 위해행위의 처벌 등에 관한 법률」은 IMO에서 1988년에 채택한 “항해의안전에대한불법행위의억제를위한협약” 및 “대륙붕상에소재한고정플랫폼의안전에대한불법행위의억제를위한의정서”의 이행법률로서 2003년 5월에 제정된 것이다. 이 법은 선박 및 해상구조물에 대한 안전한 보호와 국제테러에 대한 근본적인 방지가 목적으로 대한민국 영역외에서 발생한 대한민국 선박 및 해상구조물에 대한 위해행위를 한 외국인도 처벌할 수 있도록 관할권을 확대하고 있다. 또한 위해행위를 한 것으로 의심되는 범죄인의 인도절차 및 위해행위의 구체적인 내용도 정하고 있다.

나. 주요내용

가) 적용범위

이 법의 적용범위는 내국인, 대한민국 영역외에서 대한민국 선박 또는 해상 구조물에 대하여 이 법 위반의 죄를 범한 외국인, 대한민국 영역외에서 이 법 위반의 죄를 범하고 현재 대한민국 영역 안에 있는 외국인이다(법 제3조).

나) 범죄인 인도

대한민국 선박의 선장은 선박운항의 안전과 편의를 위하여 이 법을 위반한 것으로 의심할 만한 상당한 이유가 있는 승선중인 자를 외국에 인도할 수 있도록 하고 있다(법 제4조).

다) 범죄의 구성요건

선박·해상구조물의 안전을 해치는 살인·상해·선박납치, 위협물건의 설치, 허위정보의 전달 및 협박 등 각종 위해행위를 구체적으로 정하고 있다(법 제5조 내지 제13조).

③ SUA협약 개정의정서에 따른 국내 법률정비

가. 해상승선·검색제도 도입과 국내주관부서

해상승선·검색제도는 i) 기국의 동의절차에 따른 승선·검색, ii) 묵시적 임의승선·검색 동의, iii) 사전허용에 의한 승선·검색의 3가지가 있다. 이 중에서 사전허용에 의한 승선·검색은 불가피한 사정이 없는 한 선택할 수 없다, 묵시적 임의승선·검색 동의는 4시간내 응답이 없으면 요청국의 승선·검색에 자동으로 동의한다는 것이다. 이 제안은 체계적인 통신수단확보가 필수적이다. 우리나라는 ISPS Code 수용에 따른 선박 감시시스템이 구축되어 있어 국적선박과 체계적인 통신수단은 확보되어 있기는 하지만 4시간이라는 제한된 시간으로 국적선박에 불이익이 될 수 있다. 따라서 기국의 동의 절차에 따른

승선 · 검색이 가장 바람직하다.

나. 해상승선 · 검색제도 수행방안

SUA협약하의 범죄협의를선박에 대한 해상승선 · 검색업무 수행과 타 당사국에 의한 국적선박의 해상 승선 · 검색 요청시 대응을 위한 대응 부서가 필요하다. 현재 ISPS Code 수용에 따라 선박의 해상보안업무에 대한 해양수산부와 해양경찰청간에 통신 및 선박지원업무가 체계적으로 수립되어 있으므로 이를 활용할 필요가 있다. 따라서 해상승선 · 검색제도의 전담부서는 해양수산부로 하고, 종합상황실을 통해 선박과 요청국간의 통신업무를 수행하고, 관할영역에서 협의선박에 대한 해상승선 · 검색 및 선박지원업무는 해양경찰청이 수행하여야 한다.

다. 그 외의 고려사항

SUA협약 개정의정서의 국내수용을 위해서는 SUA협약을 수용한 선박 및 해상구조물에 대한 위해 행위의 처벌 등에 관한 법률의 내용에 다음의 내용이 고려되어야 한다.⁸⁷⁾ i) 법인에 대한 처벌 규정, ii) 정치범에 대한 인도 및 사법 공조 등을 포함한 신 범죄구성 요건, iii) BCN 무기 및 육송 등에 관한 용어의 정의, iv) 해상 승선 · 검색제도의 수용 및 그에 따른 국내 주관기관의 지정 등이 이에 해당된다.

3. 항공 · 공항 부문 보안제도⁸⁸⁾

우리나라 항공보안제도를 분석하기 위해서는 항공보안이 발전해 온 역사와

87) 정대율, “2005년 항해안전에 대한 불법 억제협약의 국내대응방안 연구”, 「해사법연구」(제18권 제1호), 한국해사법학회, 2006. 3.

88) 이 부문은 국내협동연구사업의 일환으로 유광의 교수(한국항공대학교)가 집필하였음.

항공보안의 개념을 먼저 이해해야 한다. 이와 더불어 국제민간항공기구에서 각 체약국에 요구하는 항공보안 표준에 관한 정확한 이해도 선행되어야 한다. 우리나라의 항공보안제도는 9·11테러 이후 국제민간항공기구의 항공보안감사 프로그램(USAP : Universal Security Audit Program)에 대한 대비책을 의식하면서 준비되었기 때문이다.

그러므로 이 절에서는 먼저 항공보안의 역사와 개념을 정리하고, 국제민간항공기구에서 요구하는 국가의 항공보안 책임과 항공보안활동의 중심지인 공항의 보안활동 표준을 소개한다. 그리고 우리나라 항공보안제도를 분석하고 문제점을 도출한다.

1) 항공보안의 역사와 개념

(1) 항공보안의 역사

항공보안이란 항공범죄로부터 민간항공을 보호하는 것을 의미한다. 따라서 항공보안의 역사를 서술하기 위해서는 항공범죄의 역사부터 거론해야 한다. 항공범죄는 항공운송산업의 역사 초기에서부터 발생했다. 즉, 최초의 항공기 납치 사건이 상업 항공운송업이 발아하던 시기인 1931년에 페루에서 발생했다. 페루 혁명가들이 미국 팬 암(Pan American)의 우편 항공기를 공격하여 광고물을 낙하시키는 범죄 행위를 자행하였다.

미국에서는 1930년대부터 공중 해적 행위(air piracy)도 시작되었으므로 공중 범죄 행위는 정치적 목적이든 개인적 목적이든 항공운송의 초기 단계에서부터 시작되었음을 알 수 있다. 1940년대 후반에는 공산권으로부터의 탈출을 위해 하이재킹을 이용하기도 했으며 항공운송이 급성장한 1960년대는 공중범죄도 홍수를 이루었다. 1970년대 후반부터는 국제 테러 조직 간의 협조가 시작되었으며,⁸⁹⁾ 국가조직의 지원을 받으면서 적국에 대한 테러를 수행하는 대

89) 이에 대한 대표적인 사례는 Armenian terrorist group + Red Brigades + Japanese Red Army + African Liberation Movement + Palestinians 등임.

리전쟁(surrogate warfare) 형태의 테러도 발전했는데, 리비아의 지원을 받는 테러 조직의 미국인에 대한 테러가 그 예이다.

1980년대 이후 전 세계적으로 공중 테러는 감소 추세에 들어갔다. 이는 항공보안 대책의 개선 및 각 국가들의 테러 방지 강화에 의한 결과라고 인식되고 있다. 즉, 선진국을 중심으로 각 국가들은 테러지원국을 공격하거나 경제적 제재를 가함으로써 테러 지원국의 테러 지원 활동을 약화시켰으며,⁹⁰⁾ 테러 분자나 테러 조직을 사전에 분쇄하는 작전을 사용하기도 하였으며, 특수부대를 육성하여 활용하는 대 테러 프로그램을 운영(예: SWAT, Delta Force 등)하는 등의 적극적 테러 방지 활동을 수행해 왔다.

1960년 대 말의 항공기 납치사건 급증으로 인해 1970년 대 초부터 미국을 중심으로 항공기 탑승객에 대하여 보안 검색을 수행하기 시작했다. 1974년에는 모든 국제항공여객과 기내 반입 수하물에 대하여 보안검색을 실시하는 것을 국제 표준으로 하게 되었고 (국제민간항공조약 부속서 17 채택), 각국 정부가 국가 민간항공보안프로그램을 운영하고 있으며, 공항은 통제구역, 무해지역(sterile area)을 운영하는 등, 항공보안활동이 체계적으로 수행되어 항공범죄의 건수가 점점 줄어드는 추세가 지속되었다.

그러던 중, 2001년 9월 11일, 세계를 경악하게 하는 항공범죄가 미국 뉴욕과 워싱턴에서 발생했다. 9·11 테러의 특징은 항공기를 납치하고 납치한 항공기를 무기로 지상에 있는 인명을 살상했으며 테러범이 자살을 감행하면서 테러를 수행한 점에서 지금까지는 없었던 새로운 형태의 테러로 새로운 형태의 대책을 요구하고 있다. 국제민간항공기구(ICAO)는 2002년 2월 각 체약국 정부의 고위 항공 당국자 회담을 열고 항공보안활동 관련 국제 표준을 개정하고 각국의 국제공항에 대한 항공보안 실태 감사(Audit)를 2004년부터 실시하여 2006년 현재까지 거의 완료 단계에 있다.

90) 주지하는 바와 같이, 2002년 현재 미국은 이란, 이라크, 시리아, 수단, 리비아, 쿠바, 북한을 테러 지원국으로 지목하고 있으며, 이라크를 침공 후세인 정권을 파멸로 이끌었음.

(2) 항공보안의 개념

항공보안이란 간단하게 말해 범죄 행위로부터 항공산업을 보호하려는 모든 활동을 의미한다. 항공산업 중에서도 항공운송산업이 주로 항공보안의 대상이 되며 가장 중요하게 취급되는 활동은 비행에 투입된 항공기에 대한 범죄를 예방하거나 범죄가 발생한 경우의 대응 행위이다. 항공보안에서 보호하려는 대상은 항공여객, 항공기 승무원, 지상 조업자, 일반국민 등의 생명과 항공운송활동에 투입된 재산들이다.

국제민간항공기구는 국제민간항공조약 부속서 17에서 항공보안의 개념을 다음과 같이 정의하고 있다. 항공보안이란 “국제민간항공을 범죄로부터 보호하기 위하여 인력과 물자, 대책을 종합한 것”⁹¹⁾이라고 정의하고 있다.

항공보안이 범죄로부터 민간항공을 보호하는 것으로 정의된다면 항공보안의 개념을 구체화하기 위해서는 항공범죄에 관한 개념을 구체화하는 것이 필요하다. 우선, 항공범죄의 종류를 열거하면,

- i) 항공기 납치행위(하이재킹)
- ii) 항공기 납치기도 행위
- iii) 비행중인 항공기 폭파행위(사보타지)
- iv) 공항 등 항공운송시설물 폭파행위
- v) 항공기내 범죄 행위
- vi) 기타 항공운송의 안전성을 저해하는 불법행위(예 : 운항중인 항공기내 또는 안전운항을 저해하는 농성행위, 기내난동 행위 등) 등이다.

항공기 납치행위는 일명 하이재킹으로 비행에 투입된 항공기의 승무원을 위협하여 원래 계획된 대로 비행을 하지 못하게 하면서 저지르는 범죄행위이다. 항공기폭파행위(사보타지)는 비행에 투입된 항공기에 폭발물을 장치하여 항공기를 폭파시키거나 의도적인 절차누락 등으로 비행중에 항공기가 파손되도록 하는 범죄 행위를 의미한다. 사보타지는 폭발물만 장치하고 자신은 탑승하지

91) ICAO Annex 17, Chapter 1, Definition ; A Combination of measures and human and material resources intended to safeguard international civil aviation against acts of unlawful interference.

않는 방법과 폭발물과 함께 탑승하는 자살 테러 등 두 가지 유형이 있다. 공항 시설물에 대한 폭파행위도 항공범죄 역사에 기록이 있으며 그 외에 기내에서 승무원의 통제를 따르지 않고 난동을 부림으로써 항공기 안전 운항을 저해하는 범죄행위도 자주 발생하며, 항공사 서비스에 불만을 품고 기내에서 농성을 하는 행위도 항공범죄로 간주된다.

이와 같은 항공범죄를 저지르는 사람들은 범죄조직에 소속되어 조직의 목적을 위해 범행하는 경우와 개인적인 목적에 의해 저지르는 경우로 크게 나눌 수 있다. 범죄조직에 의한 경우는 충분한 자금과 인력, 기술력을 동원하고 장기간 준비를 하며 치밀한 계획에 의해 범행을 하게 된다. 이들은 항공기를 납치하여 조직의 목적을 달성하기 위한 협상 조건을 걸고 항공기 탑승자를 인질화하여 협상을 시도하는 경우도 있고, 목표 항공기를 폭파하여 적대적 관계에 있는 국가나 조직을 위협하는 사보타지 범행을 하기도 한다. 그러나 2001년 9월 11일 발생한 미국 뉴욕 및 워싱턴 테러 행위는 항공기를 납치하여 납치한 항공기로 지상의 건물과 사람에 대해 공격을 가한 전대미문의 항공범죄 행위였으며 단순한 항공기 납치나 사보타지로 구분할 수 없는 형태이다.

반면에 개인이 저지르는 항공범죄는 범죄의 동기가 개인적이다. 금품을 강탈하기 위해서 범죄를 저지르거나, 개인적으로 망명을 기도하거나 또는, 정신병에 의해 우발적으로 사건을 일으키는 경우도 있다. 개인적인 범죄는 치밀하지 못하고, 범죄 기술과 자금력에 한계가 있으며, 인질 협상에도 한계성을 보이는 경우가 많아 사건을 쉽게 종결시킬 수 있다. 그러나 정신병에 의한 우발적인 범죄의 경우 예측 불가능한 사태가 발생할 수도 있으므로 신중하게 대처해야 할 것이다.

최근 중대한 문제로 대두되고 있는 정치적 목적을 갖는 항공테러 조직들은 테러 지원국의 지원이나, 마약, 밀수 등에 의한 방대한 자금력을 바탕으로 그룹 행동에 의한 테러를 기도하며, 첨단 기술을 테러에 응용하고, 충분한 훈련을 받은 후 정교한 방법으로 테러를 함으로써 이에 대한 효과적인 대응책의 개발이 어려워지고 있는 실정이다. 이러한 계획적인 테러 조직들의 목표와 특성은 다음과 같다.

- 국제적 관심 집중

- 정치적 선전 대중화
- 적대국가 위협
- 공권력의 무력화(無力化)
- 압력 행사
- 상징적 목표물의 공격 (9·11 테러의 경우 공격 목표는 미국으로 경제적 상징인 무역센터와 국방의 상징인 펜타곤을 공격함)

항공범죄를 막기 위한 항공보안 활동은 비행에 투입되는 항공기에 대한 납치나 폭발물 장착을 방지하는 활동을 위주로 구성된다. 따라서 항공보안은 하늘에서의 안전을 위한 대책이지만 대부분의 활동은 지상에서 이루어진다. 즉, 항공기 내로 무기나 폭발물이 반입되지 못하도록 하는 조치는 공항에서 완료되어야 하기 때문이다. 항공기내 보안 대책도 필요하지만 항공보안활동의 대부분은 공항에서 이루어져야 한다는 점이 지적된다.

2) 국가의 항공보안 책임과 공항의 보안활동 표준

(1) 민간항공보안을 위한 국가의 책임

국민의 재산과 생명을 보호할 책임이 있는 국가는 민간 항공을 범죄로부터 보호해야할 책임을 당연히 부담한다. 국가는 전반적인 민간항공보안프로그램을 수립하고 이의 실천을 위한 관련 부서의 책임과 의무를 법적 체계로 수립해 놓아야 한다. 항공보안활동에 참여하는 부서 및 기관이 많아서 책임과 의무에 대한 명확한 정의가 필요하고 보안활동에 소요되는 시설, 장비와 인력 운영에 소요되는 자원 확보 방안도 국가가 확실하게 규정해 놓아야 한다.

① 국가민간항공보안 프로그램 체계와 내용

국제민간항공조약 부속서 17에 의하여 각 체약국은 국가민간항공보안 프로그램을 수립하고 담당 정부기관을 지정한 후 이를 실천해야 한다. ICAO는 항공부서 뿐만 아니라 보안관련 일반부서의 책임과 의무를 포괄하는 국가민간항

공보안 프로그램을 수립할 것을 요구하며, 국가민간항공보안위원회, 공항보안위원회 등도 항공관련 기관뿐만 아니라 일반 보안관련 부서들도 참여시켜 구성할 것을 요구하고 있다. 따라서 항공보안에는 항공운송업의 주요 역할 담당자인, 정부의 항공당국, 공항, 항공사와 더불어 경찰, 검찰, 정보부서, 세관, 이민국, 법무부, 외무부 등이 협조 또는 특정한 역할을 해야만 한다.

국제민간항공기구는 체약국의 국내 민간항공의 안전과 보안 등에 관해서는 간섭하지 않고 국제민간항공의 안전과 질서, 효율성 증진을 고려하는 것을 목표로 하고 있음을 천명해왔다. 항공보안 측면에서도 국제민간항공의 보안활동만을 고려해왔기 때문에 부속서 17의 모든 표준과 권고 사항들은 국제공항이나 국제항공운송편에 적용하는 것으로 국한하여 기술해 왔었다. 그러나 9·11 테러 사건 이후 개정된 부속서 17에는 국내항공활동에도 국제항공에 적용되는 표준을 되도록 적용할 것을 의무화하고 있어 이제는 부속서 17의 표준을 국내 항공활동에도 적용해야한다. 이와 같은 변화는 9·11테러가 국내선을 대상으로 자행되었기 때문에 야기된 것이다.

국가민간항공보안 프로그램에는 다음과 같은 내용이 포괄되어야 한다.

〈표 5-5〉 국가민간항공보안 프로그램의 내용

- 국가민간항공보안 프로그램의 목적 및 관련국제협약 준수여부를 천명해야 한다.
- 관련기관의 책임과 권한 부여를 위한 법규 제정으로 보안활동의 합법성을 확보해야 한다.
- 국가민간항공보안 책임부서를 지정(대개, 항공국 또는 항공청) 하며 이 부서는 프로그램의 개발, 실천, 유지에 책임을 지도록 한다.
- 국가 내 항공보안 관련 부서의 책임과 의무를 명시한다.
- 항공기, 공항시설, 항행지원시설 보호 절차가 포함되어야 한다.
- 항공기 탑승자, 탑재품 보안확보 대책이 포함되어야 한다.
- 보안관련 장비의 획득, 운영, 유지 절차가 포함되어야 한다.
- 불법간섭에 대한 대응, 관리, 처리, 보고 절차가 포함되어야 한다.
- 정부와 민간항공업계에 위협수준에 응하는 보안 수준 통보 절차가 포함되어야 한다.
- 항공보안관련 국제협력 절차가 포함되어야 한다.
- 항공보안실천업무 감독, 위협대응책 준비, 보안프로그램 검토 평가 절차가 포함되어야 한다.
- ICAO에 대한 보안사고 통보 절차가 포함되어야 한다.
- 신규시설에 대한 보안대책 마련 절차가 포함되어야 한다.

또한 국가민간항공보안 프로그램을 운영하면서 프로그램의 효과를 증진시키기 위한 노력이 필요하며 이를 위해 효과 측정절차도 필요하게 된다. 효과 증진을 위해서는 운항활동 등에서 얻어지는 자료를 수집 분석하여 위협의 내용과 수준을 평가하고 위협상황에 맞는 보안활동이 이루어지도록 해야 한다. 또한, 항공보안활동에 필요한 장비, 시설, 인원 조사를 통해서 결핍 사항을 파악하고 대책을 수립하도록 하며, 최소비용으로 최대효과를 거둘 수 있는 보안체계가 적용되도록 하며, 장비, 인원, 시스템의 점검 및 결함 수정이 체계적으로 이루어지도록 해야 한다.

국가민간항공보안프로그램 운영에 필요한 재원마련의 궁극적인 책임은 정부에 있지만 정부는 항공사 및 공항에게 부담을 전가하고 사용자 부담 원칙을 적용하는 경우 궁극적으로는 항공여객이 부담하는 체제로 된다. 이 경우 실비 부담 원칙이 적용되어 보안료(security charge)로 수집된 비용은 보안활동에만 쓰이도록 해야 한다.

② 국가의 항공보안 활동

위에서 언급한대로 국제민간항공기구(ICAO) 회원 국가의 정부는 자국의 항공보안 체계 전반에 대한 책임을 지고 있다. 그러나 실제의 보안 업무 수행은 공항과 항공사 등의 책임하에 수행되도록 하고 있는 경우가 많고 미국 등 일부 국가만 정부가 직접 보안활동을 수행하고 있다. 우리나라도 정부의 항공보안 당국이 직접적인 업무수행 책임을 지지는 않는다. 승객이나 수하물의 보안 검색, 공항의 보안 구역 설정 및 운영 등은 공항공사가 책임지도록 되어 있고, 화물 보안과 항공기에 대한 보안 업무는 항공사가 책임지고 수행하도록 되어 있다.

그러나 국가는 공항이나 항공사가 수행하는 보안 업무의 품질관리의 책임을 담당하고 있다. 즉, 보안 업무가 법규대로 수행되고 보안 효과가 적당한 상태를 유지하는 지를 점검하고 불만족스러운 부분에 대해서는 시정을 지시하는 역할을 담당하고 있다. 또한, 재원 확보나 보안 인력의 품질관리, 기관간 업무

조정 등에는 법규 신설이나 개정 등을 통하여 정부가 결정적 의사 결정을 하고 있다. 정부는 보안 감독관을 두어 공항이나 항공사의 항공보안 활동을 점검 또는 감독하고 국가항공보안위원회, 공항보안위원회 등에서 주도적 역할을 하여 항공보안이 법에 따라 또는 위협 수준에 따라 적절하게 수행되도록 지도 감독하는 역할을 하고 있다. 결국 정부는 항공보안의 규제자(regulator)로서의 역할을 담당하고 있다고 보면 될 것이다.

구체적 항공보안업무들은 항공사나 공항공사 등이 수행하지만 국가적 차원의 보안 정책 수립이나 업무 조정은 당연히 정부가 수행해야 한다. 이를 위해서 각국은 ICAO 표준에 의해 ‘국가항공보안위원회’를 설치해야 한다. 국가항공보안위원회는 정기적인 회의를 갖는 상설 조직이어야 하는데 정책 및 전략을 의결하는 역할을 해야 하므로 정부기관의 고위 관리와 항공 산업계의 고위직 대표자들로 구성되어야 한다. 이 위원회의 상시적 의장직은 항공관련 정부 부서에서 담당하는 것이 바람직하며, 우발 사태가 발생하여 임시로 소집된 회의의 경우에는 우발 사태 처리에 책임이 있는 정부부서에서 임시 의장 직무를 수행하는 것이 효과적일 것이다. 이 위원회에는 정부 항공당국, 보안부대, 경찰 기관, 출입국관리소, 세관, 기타 국경통제기관, 우정국 및 국제협력기관 등이 필수로 참여하도록 해야 한다. 또한, 이 위원회가 항공전문가의 지원을 효과적으로 받도록 하기 위해서는 공항운영조직, 항공사, 항공기 승무원, 항공교통관제업무 기관, 항공통신기관의 대표자들이 특별 위원으로 참여할 수 있도록 해야 한다.

국가항공보안위원회의 책임 또는 권한은 다음과 같다.

i) 항공보안에 관한 책임 정부 당국에 대하여 민간항공과 시설에 대한 위협에 대처하기 위한 항공보안 대책에 관하여 조언한다.

ii) 보안 대책 실천이 적절히 유지되도록 지속적으로 검토하며 새로운 위협요인이 발생하면 이에 따른 보안 대책 변경 권고안을 제시하고, 항공보안 관련 기술 개발 등을 유도한다.

iii) 위협 형태 및 정도와 관련하여 국가 민간항공보안 수행 책임 부서 간 업

무 조정기능을 한다.

iv) 새로운 공항 설계 및 기존 시설 확장 설계 시 보안 사항이 고려되도록 장려한다.

v) 항공보안에 관한 책임 정부 당국과 협조하여 국가 보안 정책 변경, 법규 변경 등에 참여한다.

vi) 공항보안위원회의 권고안을 검토하고 필요시 보안계획 변경을 항공보안에 관한 책임 정부 당국에 권고한다.

(2) 공항의 항공보안 활동

① 공항보안당국 (Airport Security Authority)

공항보안프로그램의 수립 및 운영 책임은 공항 운영 조직의 보안부서가 담당한다. 공항보안부서(Airport Security Authority)의 장은 임원급으로 하여 공항장에게 직접 보고하는 지위에 있어야 하며, 공항운영과 보안 업무에 관한 일반적, 기술적 지식을 보유하고 있어야 한다. 또한 공항보안부서의 장은 공항의 모든 시설과 공항 내 타 기관의 시설에도 접근 권한이 부여되어야 하며, 공항의 보안 절차에 대한 조사 및 검사 권한과, 취약점에 대한 시정을 권고할 수 있는 권한이 부여되어야 한다.

현실적으로 공항보안부서의 장의 권한은 실무 책임자에게 위임되어 수행되겠지만, 다음과 같은 권한과 책임이 부여된다.

a) 기존의 절차에 따라 검사와 감사 및 조사를 실시한다.

b) 상기에 기술된 방식과 공식적인 양식으로 각 검사, 감사 및 조사 관련 보고를 한다.

c) 공항행정당국, 항공사뿐만 아니라 경찰당국, 우편당국 및 기타 기관 등에게 보안조치상의 문제점과 취약점에 관한 주의를 환기시키고, 보안대책 관련 권고를 한다.

d) 적절한 조치를 요하는 심각한 법적위반 사건을 보고한다.

- e) 공항에 대한 포괄적인 보안조사를 실시하고, 정기적으로 공항에 대한 감사를 실시한다.
- f) 공항계획/설계팀의 구성원으로 참여한다.
- g) 공항의 취약점을 시정하고 공항에 필요한 보안수준을 충족시키기 위해 공항보안 프로그램의 수립하고 수정한다.
- h) 문서화된 보안프로그램을 최신으로 유지하고 항공보안당국의 승인을 받는다.
- i) 보안프로그램의 효율적인 이행과 유지를 위하여 승인된 보안대책 및 절차 적용에 대한 감독을 한다.
- j) 공항당국과 기타 경찰기관과 유기적인 연락체제를 유지한다.
- k) 보안측면에서의 공항보안요원, 소방요원 그리고 구급 요원들 간 협조 체계를 공고히 하도록 한다.
- l) 공항에서 근무하는 모든 인원들에게 보안에 대한 경각심을 일깨운다.
- m) 공항보안 대책 수행하는 요원에 대한 자문을 제공하여 적절한 훈련을 받도록 한다.
- n) 승객 및 수화물에 대한 검색업무에 완벽성 및 효율성을 위해 관련 보안조사, 감사, 테스트를 시행한다.
- o) 위험요소 또는 상황발생에 효율적으로 대처할 수 있는 대응능력을 고무, 배양한다.
- p) 기존 공항의 설비변경 및 공항신축 건축물 변경시 보안요건을 반영하도록 권고한다.
- q) 민간항공과 민간항공 시설에 대한 불법 방해행위 관련 국가 법령 및 규정에 대한 지식을 가지고 이해한다. 보안기술 및 기법뿐 아니라 공항보안 책임자가 시행하여야 하는 보안조치 관련한 해당 법령과 규정에도 특별한 주의를 기울인다.
- r) 승객검색 과정에서 발견된 폭발물, 모든 무기류, 그리고 기타 위험 등을 포함해서 공항운영시 발생한 모든 불법 방해행위 사건을 기록 유지한다.

s) 불법, 강제적으로 억류되거나, 항로 이탈된 항공기 관련 제반정보를 수집하고 항공보안 당국에 송부한다.

t) 공항 이륙한 항공기가 시설 파괴를 수반한 불법적 방해행위로 인해서 납치되거나 사건과 관련되었다고 보고 접수시 관련 국가법령에 규정된 범위 내에서 조사를 즉시 실시한다. 재발방지를 위하여 어떠한 추가 보안대책이 필요한지를 파악할 수 있는 정보를 얻기 위해서 이러한 경우에는 즉각적인 조치가 필요하다.

u) 공항보안 프로그램 개발시 보안관련 사항을 조정한다.

② 공항보안위원회 (Airport Security Committee)

공항의 항공보안업무는 각종 정부부서, 항공사, 공항 및 협력 업체 등 많은 별개의 조직들이 관여하게 됨으로써 업무 조정 및 상호 협조가 긴밀하게 이루어져야 한다. 이를 위하여 통칭 공항보안위원회(airport security committee : ICAO 용어)가 필요하게 되는데 국제민간항공기구는 공항보안위원회의 역할을 다음과 같이 정의했다.

i) 국가 민간항공 보안 프로그램 시행 요건 조정 역할

ii) 공항 및 공항 사용자에게 영향을 미치는 항공보안 문제 관련 회의를 위한 장의 제공 역할

iii) 항공보안 책임당국, 국가항공보안 위원회 및 공항에서 항공보안 임무 시행과 관련 있는 직접적 책임 기관 간의 상호 연락을 취할 수 있는 수단 제공의 역할

국제민간항공기구는 공항보안 위원회를 구성할 때 다음과 같은 구성원이 포함되도록 할 것을 권고하고 있다. 국가마다 상황이 다르지만 아래에 제시한 것과 동일한 또는 유사한 기능을 가진 부서들이 참여할 수 있도록 해야 할 것이다.

a) 공항 운영책임자

b) 공항경찰의 최고 선임자

c) 각각의 보안업무 수행조직 최고 대표자

- d) 출입국 관리기관 최고대표자
- e) 공항우편당국 대표자
- f) 공항통신당국 대표자
- g) 항공 교통관제소 대표자
- h) 공항의료기관 대표자
- i) 소방 및 구조 조직 대표자
- j) 항공사 대표자
- k) 화물 운송업체 대표자
- l) 공항보안 책임자
- m) 주요 회사의 노조 대표자
- n) 필요에 따라 공항출입국 간소화 위원회 대표를 포함한 추가 참여자

③ 공항의 항공보안활동

공항에서의 항공보안 활동은 공항이 자체적으로 제정하고 정부의 항공보안 당국에 의하여 인가를 받은 “공항보안규정”에 따라 이루어 지는데, 대체로 다음과 같은 내용을 포함하여야 한다.

가. 공항지역 전반의 보안 대책

공항의 전반적 지역에서 테러, 파괴, 절도 무단침입 등의 범죄 활동이 발생하는 것을 방지하기 위한 활동이 필요하다. 우선은 공항지역의 무단접근 및 통과를 금지하기 위한 대책이 필요한데, 담(fence)을 설치하고 무단진입 및 접근을 금지시키는 경고문(warning, notice) 등을 부착하는 등의 방법이 적용된다. 의도적 무단 침입을 저지시키기 위해서는 담 안팎의 일정 공간을 잔디 및 공터로 조성하여 무단 침입자가 쉽게 발견될 수 있는 환경을 만들어야 하며, 공항운영상 필요한 출입문은 최소화하고 출입문에는 CCTV, 경비초소 운영 등을 통한 보안활동을 하거나 원거리에서 감시하는 경우는 조명을 밝게 하여 효과를 높이도록 하여야 한다.

나. 감시활동

수상한 불법행위 사건, 불법행위로 의심되는 행위에 적절하게 대처하고 수상한자에 대한 적절한 심문을 할 수 있도록 훈련받은 경찰관이 잠재적인 보안사고에도 대응할 수 있도록 항상 대기하고 있어야 한다. 터미널 내 제한구역이나 공공장소는 사복경찰 또는 공항보안요원이 공개적으로 또는 은밀하게 항상 감시를 하여야 한다. 만약 CCTV가 사용된다면, 효과가 충분하도록 하기 위하여 때에 따라서는 눈에 잘 띄는 표지판과 함께 설치되어야 한다. 쓰레기통, 계단 화장실처럼 폭발물 및 장치를 숨길 수 있는 물건이나 지역은 점검을 쉽게 할 수 있도록 설계되어야 하며, 일반적인 감시와 정기적인 점검을 받아야 한다.

다. 일반대중에 대한 항공보안 관련 공지

일반대중(공항 상주 직원 포함)은 항공보안프로그램의 일반적인 요건, 특히 여객터미널에 적용되는 보안요건과 불법 방해 행위 방지를 위한 일반대중의 역할을 알고 있어야 한다. 방치수하물 방지를 위해 일반대중이 취해야 할 기본 보안절차와 수상한 자 발견 시 즉시 경찰 및 보안요원에게 신고해야 할 의무나 신고 요령 등에 대하여 일반대중 및 승객들에게 알리기 위하여 터미널 내 안내방송시스템을 통해 정기적인 안내방송을 해야 한다. 추가적으로 여객터미널, 항공사 및 여행사 사무실 등에 적절한 안내표지를 설치 할 수 있다. 비록 많은 항공 여행 티켓들이 인터넷을 통한 통신판매나 여행사직원을 통해 구매가 이루어지고 있지만, 공항에서 항공권을 발권하는 경우도 적지 않다. 따라서 항공사 소속의 공항 상주 발권 수속 직원들도 국가항공보안프로그램에서 규정한 추가 보안 조치 또는 강화된 보안조치 대상인 자를 식별할 수 있도록 하는 훈련받음으로써 보안에서 중요한 역할을 할 수 있다. 또한, 불법행위에 사용될 수 있는 여행서류의 도난을 방지하기 위해서 발권 및 다른 수속 카운터시설은 승객 및 일반인들의 접근을 방지할 수 있도록 만들어져야 한다. 모든 티켓 및 탑승권, 환승서류 및 수하물표 같은 여행서류는 도난당하거나 잘못 사용되지 않도록 항상 보호되어야 한다.

라. 수하물처리 시스템

인가되지 않은 물품이 수하물 처리시스템으로 유입되는 것을 막기 위해서 체크인지역으로부터 수하물 분류 및 처리지역까지 있는 수하물 컨베이어 벨트는 적절한 검색 및 기타 출입통제 대책을 사용하여 보호하여야 한다. 오직 인가 받은 사람만이 유지보수 목적 등으로 수하물 처리시스템에 접근할 수 있도록 허가되어야 한다.

마. 무주 수하물 (unattended baggage)

공항터미널 내에 버려지거나 또는 일정시간 동안 주인이 없이 남겨진 무주 수하물에는 폭발장치나 다른 위험한 물질을 포함하고 있을 수 있다는 것을 모든 사람들에게 주지시켜야 한다. 그러한 가방들은 수상한 물품으로 간주하여 누구라도 경찰 또는 공항보안요원에게 신고를 하여야 하며, 경찰 또는 공항보안 요원은 이를 조사한 후 필요시 안전한 장소로 격리하여 분쇄해야 한다. 방치된 수하물 처리를 위한 시설은 처리하거나 보관하는 도중에 발생할 수 있는 폭발의 영향을 최소화 할 수 있도록 건설되어야 하고 감시요원이 없더라도 일반인의 접근이 어렵도록 설계되어야 한다. 이러한 물품은 보관소로 이동하거나 보관하기 전에 훈련된 직원에 의해 수검색 또는 X-ray 검색을 하도록 하는 규정이 마련되어야 한다.

바. 미 수취 수하물

항공기에서 하역되었으나 승객이 찾아가지 않는 위탁 수하물은 보안 조사를 해야 하고 명확히 소유주를 확인할 수 없을 경우에는 일반대중이나 직원들에게 위험을 주지 않는 장소로 이동시켜야 한다. 가능한 빠른 시간 내에 폭발물이나 다른 위험한 물건이 들어 있지 않다는 것을 확인하기 위해서 검색하거나 수 검사를 해야 한다. 이런 수하물은 소유자에게 인도되거나 현지 법률에 따라서 안전하게 처리될 때까지 침입방지시스템 또는 24시간 경비요원 경비 하에 보안성을 갖춘 저장시설에 보관되어야 한다.

사. 보안 제한 구역

보안제한구역은 비행활동의 보호를 위해 접근이 통제되는 공항의 에어사이드 지역이다. 이 지역은 주로 보안검색지점과 항공기 사이의 승객출발을 위한 절차 및 대기 지역을 포함한다. 철저한 보호라는 보안의 핵심원칙을 유지하여야 하나 가용 자원의 제한성을 고려하지 않을 수 없다. 즉, 국가는 적절히 보안성을 유지할 수 있는 보안요원들의 규모를 고려하여 적절한 규모로 보안제한구역을 유지해야 한다. 공항의 에어사이드 전체를 보안제한구역으로 설정하는 것이 가능하기도 하지만, 공항의 항공교통 처리와 직접 관련이 없는 방대한 공간을 반드시 커버해야 할지는 고려해 보아야 할 문제이다. 만약 방대한 지역을 보안제한구역으로 정할 경우, 사용 가능한 보안 자원이 급속히 분산되어 실제적으로 수행하여야 하는 효과적인 보안수준을 유지하지 못할 수도 있다.

따라서 보안제한구역은 항공기 운항규모, 보안활동에 투입할 수 있는 가용 보안요원의 수, 현 위협 분석에 따라 효과적으로 중요 목표물에 배치해야 할 자원을 고려하여 가능한 작은 범위를 유지해야 한다. 이렇게 하면, 예를 들어 에어사이드지역 주변을 이용하는 모든 차량에 대해서가 아니라 항공기에 서비스를 제공하고 접근할 필요가 있는 차량과 인원의 접근만을 허용하여 강화된 출입통제수준을 유지 할 수 있다. 추가적인 단계별 접근통제 및 보호대책이 특정 항공기에 대하여 실시될 수 있다.

아. 출입통제

보안 제한구역으로의 출입은 엄격히 통제되어야 한다. 출입지점은 최소로 하여야 하며 이 지점에는 효과적인 출입통제조치나 잠금장치가 설치되어야 한다. 직원들의 보안제한구역 출입은 업무 목적상 출입해야 할 분명한 사유가 있는 사람들로 제한되어야 한다. 보안제한구역은 계속적인 출입통제조치를 해야 하고 사용 전에 철저한 검사를 하여야 한다. 승객은 보안제한구역이나 에어사이드로 진입하기 전에 여권 등과 같은 정부발행신분증과 항공기 탑승권 또는 유효한 항공권을 제출해야겠다. 일반인이 게이트나 항공기를 통하여 항공기로

부터 도착하는 승객을 만나기 위해서 보안제한구역이나 에어사이드로 출입해서는 안된다. 모든 다른 인원들은 유효한 공항출입증을 제시하고 제한구역에 출입하도록 하여야 한다. 모든 승객과 승객 휴대수하물이나 기타 물품은 보안 제한구역으로 들어오기 전에 검색을 받아야한다. 승객 이외의 모든 기타 출입자는 정부당국이 위협에 따라서 선별적으로 검색을 수행해야 한다고 판단할 경우를 제외하고는 모두 동일한 기준으로 검색을 받아야한다. 계류장 지역 그리고 주기된 항공기로 연결되는 모든 문, 계단, 탑승교는 사용하지 않을 경우 잠금장치로 잠가야 한다. 계속적으로 감시하지 않는 비상용출입문의 경우 공항 보안 통제 센터 같은, 감독 지점에서 감시할 수 있는 영상 및 음성 경고 장치를 갖추어야 한다. 비상시 작동되는 출입문 손잡이에 파열성 장치나 덮개를 사용하면 목적외 사용을 막을 수 있다.

자. 귀빈 시설

귀빈시설을 이용하는 사람들에 대한 위협의 정도가 높기 때문에 귀빈시설에 대한 세심한 고려를 해야 한다. 귀빈과 그들의 환영 및 출국절차를 통제할 수 있는 설비를 갖추어야 하며 일반승객 처리와는 분리된 승객 체크인 처리 시설, 휴대수하물 및 위탁수하물 검색 전용시설을 갖추어야 한다. 귀빈시설을 용이하게 사용하기 위해서 랜드사이드와 에어사이드 사이에 걸쳐있을 경우 다른 출입지점과 동일한 출입통제 수준이 적용되어야 하며, 이런 시설 사용시 에어사이드와 랜드사이드의 경계의 보안성을 유지하도록 해야 한다. 귀빈시설을 사용하지 않을 때에는 안전하게 관리해야 한다.

차. 추가 보안조치

위협에 상태에 따라서, 승객, 일반인, 그리고 터미널 시설을 보호하기 위한 추가 조치들이 필요할 수 있다. 위협 수준이 높을 때 선별적으로 적용해야 하는 보안조치에는 다음의 내용이 포함된다.

- 터미널지역내와 주위에 무장한 보안요원수 증강

- 터미널 지역내와 주위에서 감시업무를 하는 사복 보안요원 수 증강
- 폭발물 탐지견 팀 순찰 횟수 증강
- 터미널의 출입초소 수 축소 및 터미널을 출입하는 인원에 대한 무작위 검색
- 터미널 진입로로 근접하는 차량과 인원에 대한 무작위 조사
- 터미널 주변 지역에 주차 금지
- 공중 수하물 저장라커의 사용 금지 또는 제한
- 폭발물을 은닉할 수 있는 터미널의 쓰레기통이나 기타 쓰레기 용기를 비우거나 제거
- CCTV감시 및 보안순찰 증강을 통한 터미널 지역의 감시수준 강화
- 일반 터미널 지역의 유리창에 방폭필름 또는 방폭커튼 설치
- 특정 위협 목표가 된 항공사의 발권 및 수속카운터를 위협하는 낮은 항공사가 이용하는 발권 및 수속 카운터로부터 분리
- 위협수준이 고조된 경우, 여객식별 위협을 줄이기 위해 공동 탑승수속 카운터 사용

카. 추가 보안자원

공항은 위협 사태 등에 대비하기 위한 우발계획(contingency plan)을 수립하고 훈련 등을 실시해야 한다. 보안대책의 향상을 위한 우발계획은 위협수준이 증가하여 추가 보안자원 준비에 대한 대책이 필요할 경우에 대비한 준비를 포함하여야 한다. 여기에는 다음 사항이 포함된다.

- 공항 내외부에 위협이 있다고 간주될 경우 시설 순찰을 위한 적절한 운송수단 및 통신장비를 갖춘 훈련된 추가 보안요원 준비
- 승객, 승무원과 공항직원을 검색하기 위해 사용된 현재의 보안시스템을 강화를 위하여 단기간의 통지로 추가적인 보안장비 구매 가능토록 조치
- 공항지역 내외에서의 보안사고 발생시 즉각적인 도움을 제공하는 해당 경찰당국과 비상대응 조직과의 협력

타. 공항 외곽지역 보호

항공기, 공항시설 및 설비들에 대한 공항경계 외곽에서의 원거리 공격에 대한 방어는 외곽지역에 대한 감시를 통해 가능하다. 이러한 감시에는 적절한 장비를 갖춘 경비요원의 공항외곽순찰과 기존에 설치된 초소에서의 감시 또는 폐쇄회로나 다른 침입 감지장치를 통한 감시를 포함한다. 수목이 우거진 지역, 주차장, 항공기의 이착륙 경로지역에 위치한 사용하지 않는 건물처럼 감시가 용이하지 않은 지역에 대해서는 각별한 주의가 필요하다. 일반적으로 위에 설치된 활주로나 유도도로 운항하는 항공기는 원거리 공격에 취약하며 이지점보다 높은 지점으로 부터의 공격에 대한 별도의 추가 물리적 보안조치가 고려되어야 한다.

공항주변에서의 항공기 사고에 대해 긴급 출입을 하기 위해 종종 “크래쉬 게이트(crash gate)”라고 알려진 긴급출입 초소가 공항 외곽 울타리에 설치된다. 이 출입구 펜스의 보안성 및 표준 요건을 유지하도록 건축되어야 하며, 사용하지 않을 때는 시건 장치를 하거나 경비요원이 배치되거나 계속적인 감시를 해야 한다. 깨어지기 쉬운 재료로 연결된 잠금장치는 보안성을 유지하며 비상시 출입을 허용하는데 매우 유용한 수단이 된다. 침입감지장치를 갖춘 원격 출입초소도 고려되어야 한다.

3) 우리나라의 항공보안제도

(1) 우리나라의 항공보안 법규 체계

우리나라 항공보안 법규체제는 우리나라가 가맹된 항공보안에 관한 국제조약과 국제민간항공기구의 요구 사항을 효과적으로 준수하고 민간항공을 범죄로부터 보호하는 것을 주요 목적으로 하여 구성되었으며 다음과 같은 법규들을 포함한다.

- a) 주요 법률 : 항공안전 및 보안에 관한 법률
- b) 항공안전 및 보안에 관한 법률 시행령
- c) 항공안전 및 보안에 관한 법률 시행규칙

- d) 보안검색교육기관지정및운영기준 (항공안전본부 고시)
- e) 항공안전보안장비 종류, 성능 및 운영기준 (항공안전본부 고시)
- f) 항공화물보안기준 (항공안전본부 고시)
- g) 항공보안감독관 업무규정 (항공안전본부 훈령)
- h) 국가민간항공보안 교육훈련지침 (항공안전본부 지침)
- i) 공항건설 및 유지보수에 관한 보안지침 (항공안전본부 지침)
- j) 국가항공보안수준관리 지침 (항공안전본부 지침)
- k) 국가보안목표관리지침 (국정원 지침)

(2) 담당조직 인력 및 예산

우리나라 항공보안 담당 정부 부서는 건설교통부 항공안전본부의 항공보안과이며, 구체적 감독업무는 서울지방항공청 및 부산지방항공청 인력 중심으로 수행한다. 정부 항공보안 조직의 인력구조는 항공안전본부 보안과에 보안과장을 포함하여 8명이 편성되어 있고 지방 항공청에 감독관 요원이 22명, 본부에 4명 등 총 26명의 항공보안 감독관이 활동하고 있다. 보안과의 행정 직원은 항공보안 정책 등 우리나라 항공보안을 계획하고 정책을 결정하며 산업에서의 실행을 감독하는 역할을 하고 있다. 감독관들은 공항 및 항공사의 항공보안 업무 실행 사태를 조사, 점검하는 역할을 한다.

앞에서 제시한 대로 항공보안업무는 공항에서 주로 이루어지고 공항에서의 항공보안업무 실천은 공항공사 책임 하에 수행된다. 우리나라의 공항운영은 인천국제공항을 운영하는 인천국제공항공사와 김포공항 및 기타 13개의 지방공항을 운영하는 한국공항공사가 책임지고 있다. 이 두 공항공사의 항공보안인력 현황은 다음과 같다. 인천국제공항은 항공여객 검색용원 640명, 경비 840명, 감독자 41명 등이 항공보안업무 서비스 제공에 투입되고 있다. 한국공항공사의 경우는 전국 공항을 통합하여 보안검색요원 602명, 경비 1,084명, 감독자 56명으로 구성되어 있다.

또한, 최근의 보안활동을 위한 정부 지원 예산은 다음 표와 같다.

〈표 5-6〉 한국공항공사 공항보안예산 지원 내용

단위 : 백만원

구 분	2002년	2003년	2004년	2005년
예산액	10,000	14,500	7,541	3,600
집행실적	9,991	8,869	7,541	3,600

자료 : 한국공항공사

〈표 5-7〉 인천국제공항공사 공항보안예산 지원 내용

단위 : 백만원

구 분	2002년	2003년	2004년	2005년
경비용역	16,900	21,110	15,745	
검색용역	50.8억 (항공사 50%지원금)	90.9억원	133.0억원	17,156
항공보안장비	5억원 (폭발물탐지기 5대)	200 (CBT 프로그램구매)	1,006	618 (X-Ray 4등)

주 : 2004사업내용 : X-Ray(4대), 이동용 X-Ray차량(1대), EOD차량, 폭발물처리 및 탐지장비, 출입증교육시스템 등

자료 : 한국공항공사

4. 철도부문 보안제도

철도는 대중이 가장 손쉽게 이용하는 교통수단이다. 철도는 오랜 기간 동안 일반 시민의 생활수단으로 활용되어 왔고, 다른 교통수단에 비해 대체로 안전하고 저렴하다는 특징을 갖는다. 그리고 철도교통의 핵심시설인 철도역은 대부분 도심 가운데 위치하고 있다. 철도역은 도시의 성장과 함께 해 왔고, 주요 도시마다 철도역은 도시의 핵심 시설로 자리 잡고 있다.

그러나 철도와 철도역은 공항에 비해 보안시설이 미비한 편이다. 철도역은 일반인의 접근이 용이하고, 철도 이용과 관계없이 철도시설 및 철도차량에 접근이 가능하다. 또 승객과 화물에 대한 보안점검 시설과 장비가 공항에 비해 매우 부족한 실정이다. 특히 우리나라와 같이 국제철도가 없고 국내용으로만 이용되는 철도의 경우 보안에 대한 문제의식은 국제철도를 가진 나라에 비해 낮은 편이다.

현재 우리나라의 철도 보안은 테러에 대비한 방호지침 형태로 되어 있으나

법률이나 시스템은 아직 준비되지 않은 상황이다. 우리나라의 철도 대테러 방호지침과 철도역의 보안실태를 살펴보면 다음과 같다.

1) 철도 대테러 방호지침

우리나라의 철도 보안은 한국철도공사에서 1차적으로 담당하고 있다. 한국철도공사는 수송안전실과 기획조정본부(비상계획팀)에서 안전 및 보안업무를 전담하고 있다. 수송안전실은 안전 계획팀, 안전관리팀, 안전조사팀 등을 두고, 철도안전종합계획의 수립 및 총괄, 직무안전보건에 관한 예방 및 지도활동, 산업안전보건업무의 종합·조정, 안전관련 교육·홍보에 관한 업무, 안전점검 및 사전 예방 활동, 위기대응훈련 계획수립 및 운영 등을 전담하고 있다. 그리고 비상계획팀은 국가비상사태에 대비한 각종계획의 수립하는 총괄업무와 함께 대테러 업무를 총괄하고 있다.

그리고 이와 같은 대테러업무는 「철도 대테러 방호지침」으로 마련되어 있다. 한국철도공사는 철도에 대한 테러위험을 사전에 예방·저지·차단하고, 철도 이용자와 시설, 장비를 보호하여 열차 안전운행을 보장하기 위해 철도 대테러 방호지침을 마련하고, 테러 대응 매뉴얼을 갖추고 있다.

철도 대테러 방호지침은 철도테러위험의 유형별로 대책을 마련한 것으로 철도공사와 그 산하소속, 철도와 관련된 경비·안전관련 용역업체, 철도시설을 사용하는 기관 및 업체에 적용하도록 하고 있다.

그리고 철도 대테러 방호지침에서는 역사, 선로시설, 차량, 차량관리단, 운행 중 열차, 기타시설 등으로 방호분야를 구분하고 주요수행 지침을 명시하고 있다. 그리고 대테러 경보단계를 청색경보(Blue), 황색경보(Yellow), 주황색경보(Orange), 적색경보(Red) 등으로 4단계로 구분하여 조치사항을 마련하고 있다.

또한 테러 상황별 대응 매뉴얼을 갖추고 만일의 사태에 대비토록 하고 있다. 매뉴얼은 폭발물 발견시, 독가스 발견시, 탄저균(생물) 발견시, 협박 전화시 등으로 구분하여 대응할 수 있도록 구분하고 있고, 방송문안도 갖추고 있다.

〈표 5-8〉 철도 대 테러 경보발령단계(요약)

단 계	표시색	경보발령요건	조 치 사 항
1단계 (관심)	청색경보 (Blue)	○ 테러에 대한 관심이 요구될 때 ○ 국외에서 교통수단 및 다중이용시설 등에 대한 테러발생 시	○ 시설물(청사, 국가중요시설, 차량기지, 변전소 등) 순찰강화 ○ 역사 맞이방, 승강장, 화장실, 쓰레기통, 역사외곽 등 취약개소 순찰강화 ○ 선로(선로, 교량, 터널 등) 및 전기(전차선, 통신, 신호 등)시설물 순회점검 강화 ○ 차량 내·외부 및 열차 출발전 안전점검 강화 ○ 테러대비 교육 실시 및 위험품 안전수송철저 ○ 유관기관과의 협조체계 유지 및 비상연락망정비
2단계 (주의)	황색경보 (Yellow)	○ 건교부, 국정원, 경찰 등에서 철도를 적시하지 않고 포괄적인 테러정보를 접수한 경우	○ 1단계(청색경보) 조치사항 시행 ○ 간부급의 관내 시설에 대한 순찰 강화 ○ 필요시 유관기관과 합동으로 시설물 안전 점검 실시 ○ 테러대비 교육·훈련 실시 ○ 소속장 비상연락체계 유지
3단계 (경계)	주황색 경보 (Orange)	○ 건교부, 국정원, 경찰 등에서 철도를 적시하지 않으나 테러 징후가 높은 경우 ○ 협박전화 및 의심 물질 발견 시 (해당소속)	○ 2단계(황색경보) 조치사항 시행 ○ 지역본부장 및 소속장은 관할 구역에 대한 특별 안전점검 실시 ○ 경찰, 국정원 등 유관기관 지원요청 ○ 역구내 및 열차 내 대 테러 홍보방송 실시 (역 : 1일 3회 이상, 열차 : 1회 이상) ○ 대 테러 대책본부 운영 준비 ○ 소속장 관할구역 내 위치 및 근무필요시 직원 연장근무 조치
4단계 (심각)	적색경보 (Red)	○ 건교부, 국정원, 경찰 등에서 철도를 적시한 테러위험 정보를 접수한 경우 ○ 국내에서 철도가 아닌 타분야에서 테러가 발생한 경우	○ 3단계(주황색 경보) 조치사항시행 ○ 지역본부장은 관할 구역에 대한 총괄 지휘 ○ 소속장은 관할 구역에 대한 안전점검 1일1회 이상 실시 ○ 대 테러 대책본부 운영 (본사, 지역본부 및 소속별) ○ 유관기관 합동근무 실시 ○ 역구내 및 열차 내 대 테러 홍보방송 실시 (역 : 1일 5회 이상, 열차 : 2회 이상) ○ 승객 이용통로를 제한적 운용과 역구내 물품 은닉 가능시설 및 공간폐쇄 ○ 소속장 정위치 근무

2) 철도 역사의 보안 시스템⁹²⁾

철도 역사는 소위 ‘불특정 다수’라 일컬어지는 많은 사람들이 오가는 곳이다. 특히 전 세계적으로 테러의 공포가 확산되고 있는 상황에서 역사에 대한 보안·안전대책을 수립하는 일은 매우 중요하다. 그 가운데서도 열차와 역사 내 상황을 관리하고 있는 관제센터는 최첨단의 출입통제 시스템을 갖추고 외부의 출입을 철저히 차단해야 한다.

우리나라에서 철도 역사의 보안은 다음과 같은 형태로 이루어지고 있다. 아직 일부 역사에서만 실시되고 있으나 전국의 주요 역으로 확대되고 있다.

① 역사 내부 감시체계

역사 내에서 열차를 타기 위해서는 진입로를 건너야 한다. 이 진입로에서는 역사 관리자들이 근무하면서 역사 내 상황을 수시로 점검하며, 문제가 발생할 경우 관제센터로 즉시 통보할 수 있도록 했다.

〈그림 5-5〉 철도역사 내부전경



92) 보안뉴스 자료 참조

② 역사 출입구 감시망

역사 안으로 들어가는 모든 출입구에는 CCTV 카메라가 설치돼 이곳을 드나드는 사람에 대한 모니터링이 가능하다. 수많은 열차이용객들이 다니는 출입구인 만큼 CCTV 카메라는 돔형으로 설치해 열차이용객들이 CCTV 카메라에 대해 느끼는 부담감이나 거부감을 줄이는 것도 중요하다.

〈그림 5-6〉 역사 출입구 감시 시스템



③ 모니터링 장비

고속철도 역사의 관제센터에서는 역내를 비롯해 외부 철로 등 주요지역에 설치된 CCTV 카메라를 통해 역내 상황을 실시간 모니터링하고 있다. 특히, 철로가 2개 이상으로 분리되는 지점은 다른 철로에 비해 사고 위험이 높기 때문에 집중적으로 감시되고 있다는 게 역사 측의 설명이다.

〈그림 5-7〉 역사 감시 모니터 장비



④ 지문인식 및 카드 키 방식의 출입통제 시스템

고속철도 역사를 총괄적으로 관리하고 있는 관제센터 내부에 출입하기 위해서는 철저한 출입인증 과정을 거쳐야 한다. 그리고 관제센터 내부에서 다른 구역으로 이동하기 위해서는 카드키 방식의 출입통제 시스템을 다시 한 번 거쳐야 한다.

〈그림 5-8〉 출입구 지문인식 시스템



〈그림 5-9〉 카드키 출입통제시스템



⑤ 실내외 CCTV 카메라

열차이용객들의 안전을 위해 선로 옆에 설치된 CCTV 카메라. 이 카메라는 승객들의 이동상황을 살펴보기에 용이하며, 이용객들이 많은 복잡한 상황에서 발생할 수 있는 범죄나 도난사고 예방에 효과적이다. 역사 내 통제구역에 출입하기 위해서는 입구에 부착된 초인종을 눌러야 한다. 이 때 통제구역 내부에서는 문 윗부분에 설치된 CCTV 카메라로 초인종을 누른 사람의 모습을 확인한 후에야 출입을 허가하게 된다. 역사의 주차장에도 CCTV 카메라가 설치돼 차량의 주차상태를 파악하고, 혹시 발생할지 모를 사고나 범죄에 대비할 수 있도록 했다.

〈그림 5-10〉 역사 실내외의 각종 카메라



제6장

우리나라 물류보안제도 문제점과 정책방향

1. 우리나라 물류보안제도의 문제점

1) 물류보안제도 수용상의 문제점

우리나라의 경우 물류 시스템 전반적으로 두 가지 현안이 시급한 해결과제로 등장하고 있다. 첫째는 통합적인 물류보안 시스템이 없다는 점과 둘째는 물류보안장비 및 기술 개발에 너무 등한시하고 있다는 점이다. 특히 미국의 경우 물류보안을 강화하면서 물류보안을 확보하는데 현실적으로 필요한 장비 및 기술개발 등에 적극 나서고 있는 점은 우리나라의 현실과 크게 대비되고 있다. 이 같은 현상은 우리나라가 그 동안 물류보안 문제에 대해 수동적인 자세를 견지한데도 원인(原因)이 있지만 관련 기업들도 투자를 소홀히 한데도 원인(遠因)이 있는 것으로 분석된다.

또한 우리나라의 경우 다른 나라에 비해 최근에 들어서야 비로소 물류보안을 확보하는 정책을 추진하기 시작하였다. 해양수산부가 최근 국제선박 및 항만 시설 보안에 관한 법률의 제정작업을 추진하고 있으며, 항만운영과는 항만 보안체계 정비 및 보안역량 강화방안을 추진하고 있다. 또한 같은 해양수산부 동북아 물류추진기획단은 국제적으로 강화되는 물류보안 추세를 우리나라 항만 경쟁력 제고에 활용하는 방안 검토하고 있다. 정보화담당관실도 2005년부터 3년 동안 전자 태그(RFID) 구축사업을 시행하고 있다. 관세청은 ‘파트너 관리 시스템(C-APM)’을 구

축하고, 2010년까지 시행한다는 방침을 정해 놓고 있다.

(1) 통합적인 물류보안정책의 미비

우리나라의 경우 화물 공급망 전반을 통합적으로 관리하는 물류 보안 제도가 구축되어 있지 않다. 미국의 C-TAT의 경우 제품 생산에서 판매에 이르는 전 구간의 완벽한 보안 확보를 요구하고 있으며, 유럽연합이나 싱가포르 등도 이 같은 추세에 따르고 있다. 특히 우리나라의 경우 물류 보안 장비 및 기술개발과 투자, 협력을 소홀히 함에 따라 향후 국제 표준 경쟁에서 낙오될 가능성도 배제할 수 없다.

더 큰 문제는 국제적으로 물류보안제도가 강화되고 있음에도 일부 부처와 기업을 제외하고, 이 같은 움직임을 제대로 파악하지 못하고 있다는 점이다. 이에 따라 물류 보안을 강화할 수 있는 민관 협력 프로그램이 부족하고, 전문가 양성이나 국제 협력 등에 전혀 관심을 기울이지 못하고 있는 실정이다.

이 같은 우리나라의 통합적인 물류보안정책의 부재는 인근 국가의 발빠른 대응과 대조를 보이고 있다. 싱가포르와 홍콩, 일본, 중국 등은 자국의 보안기준을 글로벌 기준에 맞추는 한편, 이 같은 흐름을 적극 활용, 환적 화물 유치하는 물론 궁극적으로 국제 경쟁력을 높이는 지렛대로 활용하는 전략을 추진하고 있다.

(2) 물류보안시장에 대한 관심 결여

물류보안시장이 향후 새로운 성장산업으로 떠오르고 있다. 물류 전구간의 완벽한 보안 시스템을 구축해야 하기 때문에 앞으로 시장 규모가 상당히 커질 것으로 전망되고 있다. 컨테이너 보안 표준을 확보하기 위해 글로벌 기업들이 경쟁이 치열한 것도 바로 여기에 이유가 있다. 컨테이너 화물에 대한 검색기 시장뿐만 아니라 기업에 대한 보안인증 및 물류보안 컨설팅, 물류보안 전문가 육성 및 교육에 이르기까지 물류보안 시장을 크게 확대될 수 있다.

① 컨테이너 보안표준 확보에 미흡

최근 세계적으로 물류보안이 강화되면서 글로벌 업체를 중심으로 컨테이너 보안장비 사업에 뛰어드는 기업이 늘어나고 있으며, 선두 대형업체들이 이 같은 시장을 양분하고 있는 것으로 나타났다. 이 같은 경향은 앞으로 북한의 핵 실험 강행과 미국의 항만 보안법(SAFE Port Act) 채택 등으로 더욱 가속화될 전망이다.

현재 전자 태그(RFID)를 핵심으로 하는 컨테이너 보안장비 시장은 미국의 군수업체인 록히드 마틴 그룹과 GE 연합체로 나뉘어져 있는데, 두 진영은 자체적으로 개발한 시스템을 상용화하기 위해 치열한 경쟁을 벌이고 있다. 록히드 마틴의 자회사인 사비 네트워크는 최근 미국의 버지니아 항만당국과 컨테이너 보안 시스템을 설치하는 계약을 맺었다. GE는 자사 시스템인 ‘컴머스가드(CommerceGuard)’의 해외 판매망을 확정하는 등 시장 선점에 적극 나서고 있다.

우리나라 삼성물산도 최근 미국의 GE가 설립한 컴머스가드의 지분 10%를 인수하는 방식으로 컨테이너 보안 시장에 진출하였다. 삼성은 1,500만 달러를 투입, 이 회사의 지분을 인수하면서 ‘컴머스가드’의 아시아 12개 국 판매권을 확보하였다. GE는 독일의 지멘스와 일본의 미쓰비시 등과 함께 공동전선을 형성, 컨테이너 보안업체의 대표주자로 나서고 있다. 삼성은 최근 발표한 자료에서 “보안사업은 이제 국제적인 메가 트렌드”라고 강조하고, 앞으로 이 시장의 규모가 30억 달러에 이를 것으로 전망하였다.

GE가 삼성을 끌어 들여 컨테이너 보안시장에 대한 참여를 확대함에 따라 동종 경쟁업체인 Savi Networks를 갖고 있는 록히드 마틴의 향후 대응도 관심을 끌고 있다. 사비는 세계 최대의 컨테이너 터미널 운영업체인 허치슨 포트 홀딩스(HPH)가 지분을 투자한 기업으로 그 동안 허치슨 터미널을 중심으로 컴머스가드와 유사한 시스템을 구축해왔다. 이 회사가 개발한 컨테이너 보안장비 시스템은 버지니아 항만 이외에 우리나라 허치슨 터미널과 홍콩, 로테르담, 펠릭스토우 항만 등에 설치돼 있다. 이와 함께 사비는 최근 중국의 전파 규칙

위원회(SRRC)로부터 전자 태그 제품의 중국 내 사용 권한을 승인받았다. 이에 따라 사비가 개발한 전자 태그 하드웨어는 국제표준기구(ISO)의 전자 태그 기술표준(ISO 18000-7)으로 인증 받을 수 있는 전기를 마련했다는 평가이다.

글로벌 기업들이 이와 같이 컨테이너 보안 표준을 확보하고, 시장을 선점하기 위해 치열하게 경쟁하고 있으나 우리나라는 이 같은 시스템과는 다른 독자적인 시스템을 개발, 시험 운영하고 있어 이들 업체와의 경쟁에 관심이 모아지고 있다. 우리나라가 현재 시범사업을 진행하고 있는 전자 태그는 기본적으로 항만운영 효율화 사업에 목적을 두고, 출발했기 때문에 국제적인 표준에 적합한지 여부는 아직 속단할 수 없는 실정이다. 그러나 한 가지 분명한 점은 컨테이너 보안 장치에 관한 한 전자 태그 시스템보다는 컨테이너 내부에 부착하거나 컨테이너에 직접 삽입하는 시스템이 향후 시장을 선도할 가능성이 크다는 점이다. 컨테이너 보안 장비를 어느 방향으로 끌고 가야 할지 결정해야 한다.

② 컨테이너 화물 검색기 시장 상실 우려

항만 터미널에서 컨테이너 화물의 검사와 관련하여 현재 사용되는 장비는 크게 두 가지로 구분되고 있다. CSI에 따라 2002년부터 설치되기 시작한 일반적인 컨테이너 화물 검사기와 2004년부터 미국 에너지부 주도하게 설치되고 있는 컨테이너 화물 방사능 탐지기가 그것이다. 컨테이너 화물 검사기는 화물 스캔에 사용하는 촉매물질의 종류에 따라 i) 엑스레이(X-ray)형 검사기와 ii) 감마레이(Gamma-ray)형 검사기 등 2가지가 있다. 또한 설치 방식에 따라 고정식과 이동식 2가지로 구분되는데 각각 장단점이 있다.

MPI가 도입되기 전까지 세계 컨테이너 항만에서는 컨테이너 화물 검사기가 주로 설치되었으나 앞으로는 방사능 검사기까지 동시에 설치해야 할 것이다. 다만, 문제는 이 같은 시스템을 각각 별도로 설치·운영할 것인지 아니면 통합 시스템을 활용하거나 개발해야 할지 결정해야 한다는 점이다. 운영의 효율성과 설치 장소 문제 등을 고려할 경우 통합 시스템이 점차적으로 범용화될 것으로 예상된다. 홍콩 항만당국은 수출되는 모든 컨테이너 화물을 검사한다는 방침

아래 2년 전부터 초고속·초정밀 컨테이너 검사 장비를 모던 터미널에서 시험 운영하고 있다.

이 시스템은 세계 최대의 컨테이너 검사장비 제작 및 공급업체인 미국의 SAIC사가 설계한 것으로, 일반 컨테이너 검사기능과 방사능 탐지기능이 통합된 것이 특징이다. 지난 3월 미 상원 청문회에서 일부 의원들은 SAIC사의 ‘통합 컨테이너 검사시스템(Integrated Container Inspection System : ICIS)’을 승인하자고 주장했으나 국토안보부는 아직 이 시스템을 도입하기에는 이르다는 입장을 표시하였다.⁹³⁾

우리나라 항만에는 2006년 8월 31일 현재 모두 8기의 컨테이너 화물 검사기가 설치되어 있는데, 해마다 1-2기씩 추가 설치할 계획이다.

〈표 6-1〉 우리나라 컨테이너 화물 검사기 설치 현황

설치 항만	설치 대수
부산항	3(1)
울산항	1
광양항	1
평택항	1
인천항	2
군산항	(1)

주 : ()안은 올해 중 설치 예정
자료 : 관세청

우리나라에 설치되어 있는 컨테이너 화물 검사기는 미국 BIR사와 중국의 뉴텍사 제품이며, 차량 이동식 컨테이너 화물 검사기는 미국의 Lapiscan사 제품이다. 다만, 이 같은 컨테이너 화물 검사기의 핵심 기술은 가속기 제조업체인 미국 테리안사가 갖고 있다. 각 항만 컨테이너 화물 검사기의 처리 속도

93) ICIS가 생성한 이미지 파일을 정확하고, 신속하게 관독할 수 있는 프로그램이 개발되지 않았고, 다른 화물 정보와 통합 등에 문제가 있기 때문인데, 현재 이 시스템에서 생성된 자료를 읽는 데는 4~6분 정도 소요.

는 1기당 3분 정도이며, 가격은 고정식이 100억 원, 그리고 이동식이 40억~50억 원 정도이다. 홍콩 모던 터미널의 통합형 컨테이너 화물 검사기는 차량이 정차하지 않은 상태에서 검사하는 장비이며, 처리 속도는 16Km/h에 달하기 때문에 시간당 컨테이너 적재 차량 300대의 검사가 가능하다.

〈표 6-2〉 전국 컨테이너항만의 화물검색기 조달현황 및 재원

입찰년도	형식	투과력 (철판 mm)	제조사	낙찰가 (백만원)	설치항	비고
2002	조립이동식	250	Rapiscan	4900	인천항	
2002	조립이동식	250	Rapiscan	4900	부산항	
2002	조립이동식	250	Rapiscan	4900	부산항	
2002	차량이동식	150	Nuctech	2614	부산항	
2003	조립이동식	300	Nuctech	4498	평택항	
2003	조립이동식	300	Nuctech	4498	광양항	
2004	양방향 고정식	380	BIR	10355	인천항	
2004	조립이동식	300	Rapiscan	5058	울산항	
2005	양방향 고정식	380	BIR	10494	부산항	
2005	차량이동식	250	L3 Comm.	4499	군산항	설치중
2006	조립이동식	380			인천항	입찰중

자료 : 한국해양수산개발원

우리나라는 이 같은 컨테이너 화물 검사기를 도입하면서 국산 장비를 검토했으나 관세청에서 요구하는 기술 수준(사양)에 적합하지 않아 입찰자격을 주 어지지 않았다. 따라서 우리나라 컨테이너 검사기에 관한 기술 수준은 다른 나 라에 비해 상당히 열위인 것으로 판단된다. 우리나라가 제때 대응하지 못해 컨 테이너 화물 검색기 시장을 외국에 내주고 있다는 비판도 나오고 있다.

2) 운송 모드별 문제점

(1) 해운·항만 분야

① 항만별 일원화된 경비·보안업무 수행체제 미비

통합방위법 등 보안관련 법령에 의하면 국가중요시설의 경비·보안책임을 시설의 소유자 및 관리자(이하 “시설주”라 한다)에게 부담시키고 있다(통합방위법 제15조의 2). 이에 따라 항만시설의 경우도 항만시설의 소유자와 관리자가 보안책임을 지므로 부두의 소유 및 관리형태에 따라 보안주체가 달라진다. 먼저 국가가 소유 및 관리하는 항만시설의 경우는 국가가 경비보안책임을 지며, 국가로부터 항만시설을 무상대부받아 관리·운영하는 부산항만공사나 인천항만공사는 공사가 경비보안책임을 진다.⁹⁴⁾ 부산신항이나 광양컨테이너 터미널 등과 같이 민간이 소유 및 운영하는 항만은 민간 운영사가 경비보안책임을 진다. 한편, 국가는 항만시설을 임대할 수 있고, 항만공사도 국가로부터 무상대부받은 항만시설을 전대할 수 있다.⁹⁵⁾ 이 경우 경비보안책임을 임차인에게 있는지 아니면 임대인에게 있는지가 논란이 될 수 있다. 통합방위법은 국가중요시설의 경비·보안책임을 시설의 소유자 또는 관리자(이하 “시설주”라 한다)에게 부담시키고 있으나(제15조의 2), 관리자의 범위에 대한 명확한 규정이 없기 때문이다. 그런데 “항만경비및보안관리지침⁹⁶⁾”은 지방해양수산청장에게 관할항만 전체에 대하여 경비·보안책임을 지우면서 항만보호구역에서의 민유

94) 항만공사법 제8조(사업) ①공사는 다음 각 호의 사업을 행한다.

1. 「항만법」 제2조제6호의 규정에 따른 항만시설(외곽시설·임항교통시설 등 대통령령이 정하는 항만시설을 제외한다)의 신설·개축·유지·보수 및 준설 등에 관한 공사의 시행 및 항만의 경비·보안·화물관리 등 항만의 관리·운영에 관한 사업

95) 항만공사법 제28조 (국·공유재산의 전대 등) ①공사는 항만시설의 효율적인 관리·운영을 위하여 필요한 경우에는 제27조의 규정에 따라 대부받은 국·공유재산을 전대할 수 있다.

96) “항만경비및보안관리지침”은 보안업무규정과 통합방위지침(대통령훈령 제28호)의 규정에 의하여 국가보안목표시설로 지정된 항만보호구역의 경비 및 보안관리에 필요한 사항을 규정하기 위하여 해양수산부 장관이 작성한 지침임.

시설주 및 항만시설 임대계약자가 전용사용하는 시설에 대하여는 그 책임하에 경비·보안업무를 수행하도록 규정하고 있다(제3조 제1항). 이에 따라 민간이 소유·운영하는 시설과 국가 또는 항만공사가 전(임)대한 시설은 민간운영자 또는 전용운영자가 경비보안책임자가 된다. 그러면서 지방해양수산청장을 관할 항만의 경비본부장으로 지정하고, 당해항만의 경비보안에 관한 지휘체계의 일원화 의무도 부여하고 있다(제3조제3항). 그러나 경비보안본부장인 지방해양수산청장과 전용사용시설 또는 민간운영시설의 경비책임자 간의 책임관계는 명확하게 규정하고 있지 못하여 지방해양수산청장은 관할 항만에서 실질적으로 일원화된 지휘체계를 구축할 수 있는 근거가 부족하다. 경비보안체제를 구축하기 위하여 필요한 인력과 장비를 갖추기 위해서는 비용이 필요하며, 그 비용을 수혜자인 항만 임(전)차인에게 부담하기 위해 “항만경비및보안관리지침”에서 항만시설의 경비보안주체를 항만시설 소유자 또는 관리자에 한하지 않고, 항만시설 임(전)차인에게 무리하게 확대한 결과이다. 그러나 경비보안주체와 비용부담주체는 엄밀히 구분되어야 하고, 항만시설 임(차)인은 경비보안에 소요되는 비용부담의 주체임을 명확히 할 필요가 있다.

특히 ISPS Code에서 요구하는 항만 경비보안책임자는 단순히 항만시설에 대한 경비보안책임자에 그치지 않고 화물을 포함한 항만물류에 대한 경비보안책임자의 성격을 지니고 있다. 이는 ISPS Code의 시행으로 항만 경비보안책임자의 성격이 기존의 단순한 시설에 대한 경비보안책임자로서의 역할에서 전 항만의 물류에 대한 경비보안책임자로 그 성격이 변화되었음을 의미한다. 따라서 항만의 경비보안책임자는 개개의 시설 소유자가 아니라 전 항만의 물류책임자인 지방해양수산청장이어야 하며, 항만별 경비보안체제는 당해 관할 지방해양수산청장을 경비본부장으로 일원화된 지휘체계 구축이 필요하다.

② 경비·보안인력 수급체제 문제

미국의 9·11 항공기 테러 이후 국제해사기구(IMO)는 해상과 항만에서의 보안강화를 위해 2002년 12월 12일에 “국제선박및항만시설보안규칙(ISPS

Code)”을 채택하였으며, 이 규칙은 2004년 7월 1일부터 국제적으로 시행되고 있다. 우리나라에서는 ISPS Code 발효시기에 맞추어 국내 이행법률을 제정하여 시행하여야 하나 법률제정 시간의 촉박함으로 부득이 2003년 10월에 이 규칙의 국내이행을 위한 「선박및항만시설보안에관한규정(고시)」을 제정하여 시행하고 있다. 그러나 고시는 ISPS Code를 시행하는 데 따른 필수사항에 대해서만 규정하고 있어 선박과 항만 등의 안전과 보안을 위한 종합적·포괄적인 규범으로서의 역할은 미흡한 실정이며, 선사나 항만시설 운영자 등에게 부과하고 있는 의무사항도 강제집행 수단이 없어 규정의 실효성 확보에 한계가 있다.

〈표 6-3〉 각 지방해양수산청별 ISPS Code 적용대상 항만 현황

구분	대상항만	
	국가보안목표시설	ISPS Code 대상 항만
인천청	인천항	인천항
평택청	평택항, 대산항	평택항, 대산항, 태안항, 보령항
군산청	군산항	군산항, 장항항
목포청	목포항	목포항, 완도항
여수청	광양항	광양항, 여수항
제주청	제주항	제주항, 서귀포항
마산청	마산항	마산항, 진해항, 삼천포항, 통영항, 고현항, 옥포항, 장승포항
부산청	부산항	부산항
울산청	울산항	울산항
포항청	포항항	포항항
동해청	동해항	동해항, 묵호항, 속초항, 삼척항, 옥계항
계	18개 항만	28개 항만

자료 : 해양수산부

이에 여러 법령에 산재되어 있는 항만 경비보안업무의 효율성을 제고하기 위하여 「국제항해 선박 및 항만시설의 보안에 관한 법률」 제정을 2007년 6월

을 목표로 추진하고 있다.⁹⁷⁾ 한편 통합방위법, 국가보안목표관리지침 등 보안 관련법령에 의하면 국가보안목표 시설은 13개 항만이며, 경비보안이 긴요한 항만 5개를 포함하여 총 18개 항만인 경비보안대상 이었다. 그러나 2004년 7월 발효한 ISPS Code 적용대상 항만시설은 국제항해에 종사하는 여객선, 총톤수 500톤 이상의 화물선, 총톤수 500톤 이상의 어획물운반선 및 이동식 해상 구조물이 이용하는 항만시설이다.

따라서 우리나라 28개 무역항이 전부 대상 시설이며, 그 중에는 국가보안목표시설로 지정되지 아니한 10개 항만도 포함되어 있다.

그러나 ISPS Code 시행에 의해 추가로 경비보안 대상항만이 된 10개의 무역항은 경비인력 배치가 전무하고, 기존 18개 항만도 ISPS Code 시행 이후 업무증가로 인력이 부족하다.

해양수산부에서 조사한 바에 따르면 전체 항만 경비보안 소요인력은 2,647명이나 현재인원 2,383명으로 264명이 부족한 것으로 나타났다(<표 6-4>참조). 현재의 항만 경비보안주체별로 인력을 살펴보면 민간과 항만관리법인은 소요인력 대비 부족인력이 각각 3.1%(45명)과 9.3%(54명)으로 비교적 양호한 편이나 국가는 27.7%(165명)로 인력부족이 심각한 실정이다.

〈표 6-4〉 각 보안주체별 인력 현황

단위 : 명

보안주체	소요인원		현재인원				부족인력
	항만	인원	합계	청경	특경	일반	
국가	28	596	431	431	0	0	165
항만관리법인	2	579	525	474	51	0	54
민간	14	1,472	1,427	467	891	69	45
합계	28	2,647	2,383	1,372	942	69	264

자료 : 해양수산부

97) 이 법률안은 2006년 10월 18일에 국회에 제출되었음.

경비보안인력 구성을 보면 청원경찰이 1,372명(58%)으로 특수경비원 942명(40%)보다 많다. 그러나 보안주체가 민간인 경우는 청원경찰이 467명(33%)인 반면 특수경비원은 891명(62%)로 특수경비원의 비율이 청원경찰의 2배이다.

따라서 추가적으로 ISPS Code의 적용을 받는 10개 부두에 대한 인력확보와 병행하여 정부가 경비보안 주체인 항만의 인력운용의 유연성 확보를 위해 특수경비원제도를 도입할 필요가 있다. 이 경우 문제점으로 지적되고 있는 저임금으로 인한 이직률 감소대책이 필요하다. 이직률 증가는 경비보안업무의 연속성과 전문성 확보곤란으로 이어지기 때문에 단순한 인건비 절감이 특수경비원제도의 도입사유가 되어서는 안 된다. 또한 특경비원제도를 도입할 경우 기존 청원경찰과의 조화로운 운영도 풀어야 할 숙제이다.

③ 물류보안 시설 및 장비의 확충 미흡

항만 시설의 보안장비는 외곽울타리 및 CCTV, X-ray 검색기, 문형탐지기, 폭발물 탐지기, 순찰차량 등이 있다. 우리나라는 주요항만은 외곽 울타리나 CCTV 등은 항만시설 경비보안을 위한 장비는 대체로 잘 갖추어져 있으나 물류보안을 위한 장비는 절대적으로 부족하다. 또한 항만시설의 경비보안 장비도 국가가 운영하는 항만과 민간이 운영하는 항만 간에는 차이가 많다. 민간이 운영하는 항만은 준공초기부터 항만시설 보안확보 기준에 따라 시설과 장비의 확보와 체계적인 유지·보수가 잘 이루어지고 있으나⁹⁸⁾ 국가운영항만은 예산의 경직성으로 관련 기준이 요구하는 시설 및 장비확보에 어려움이 있다. ISPS Code의 시행으로 항만시설 보안위주에서 물류보안이 중시되면서 시설·장비의 부족은 심각하다. 부산과 인천이외에 항만에서는 보안의심자나 의심물품의 검색이나 추적수단은 경비인력에 의한 육안 검색과 저성능의 차량(자전거, 오토바이)에 불과하다. 연차별 계획과 항만별 선택과 집중적인 투자로 항만시설보안을 위한 보안울타리 등의 유지보수와 경비보안 종합경비상황실의

98) 민간운영부두에서 항만보안시설 확보에 소요된 비용은 인천 송도 LNG 터미널(15억), 삼천포 한전 부두(13억), 울산 SK부두(20억), 부산신항(35억) 등임.

확대 구축이 필요하다.⁹⁹⁾ 아울러 전국무역항에 대한 물류보안장비인 X-ray 검색기, 문형탐지기, 폭발물 탐지기, 순찰차량 등의 구입에 필요한 예산을 배정하여야 한다. 북한 핵실험과 관련하여 부산, 인천 및 광양항 등에는 방사성 탐지기의 구비도 고려할 필요가 있다.

(2) 항공·공항 분야

우리나라 항공보안제도는 국제민간항공기구와 미국의 제도를 대부분 수용하고 있는 현실이다. 이 과정에서 우리나라 현실에 맞지 않은 제도가 법률로 제정된 부분이 없지 않다.

특히 본 연구진의 관련기관 및 업계 면담조사¹⁰⁰⁾ 결과, 정부의 항공보안조직 문제, 보안제도 시행상의 문제, 테러기술의 발전과 대응기술 등의 문제가 있는 것으로 분석되었다. 특히 항공화물 검사시 외국선사의 검사 능력 문제, 항공 보안검색의 가장 적절한 방법으로 거론되는 상용화주 문제, 보안경비요원 문제 등과 같이 항공 보안문제는 법과 현실의 괴리에서 발생하는 문제가 상당히 존재하고 있다. 이하에서는 이에 대해 상술한다.

① 정부의 항공보안 조직 미비¹⁰¹⁾

가. 정부의 항공보안 조직 미비

우리나라의 항공보안 정부 조직은 건설교통부 항공안전본부 항공보안과와 지방 항공청의 항공보안과가 우리나라의 항공보안 시스템을 지휘 관리하는 체계로 이루어져있다. 구성원도 불과 수 명 정도로 이루어져 있어 세계 10위권인 우리나라 항공운송규모에 비교하면 턱없이 부족한 실정이다. 미국의 경우는 말할 것도 없고 많은 나라에서 9·11 이후 항공보안 정부 조직을 “청”이나 “국”

99) 현재는 부산항 및 인천항에만 경비보안 종합상황실이 있음.

100) 본 연구진은 이 부분의 조사를 위해 항공사(국적 및 외국), 정부기관, 정부업무위탁기관, 공항공사(공단) 등의 임직원을 직접 면담하였음.

101) 이 부분은 협동 연구과제(유광의 집필) 내용을 수정, 보완한 것임.

수준으로 유지하고 있는 것과는 대조적이다. 주지하다시피 항공보안은 범죄에 대한 대책이므로 정부의 역할이 커질 수밖에 없는데 왜소한 조직으로 효과적인 결과를 기대하기는 어려울 것이다. 특히, 선진국에서 중점적으로 정부가 주도하고 있는 R&D나 교육 훈련 프로그램 개발 등에는 노력을 기울일 여지가 전혀 없는 실정이다.

나. 외부 부서와의 협조 및 업무 조정 문제

항공보안 활동은 주로 공항에서 이루어진다. 공항운영업무에는 많은 기관과 부서들이 관련되어 있으며 항공보안업무 역시 세관과 경찰을 포함한 정부의 여러 부서 및 항공사, 공항당국, 하청업체 등이 관련되어 있다. 따라서 효과적인 항공보안확보에는 관련 부서들 간의 협조가 필수적이다. 우리나라는 일반적으로 부서 간 협조나 기관 간 의사소통이 원활하지 못한 문화가 문제되는 경우가 많다. 항공보안에 있어서도 기관이나 부서가 다른 경우에 적극적 의사소통뿐만 아니라 규정에 있는 정보교환도 원활하지 못하다는 의견을 듣고 실감한다. 특히, 경찰은 보안활동의 효과를 확실히 하는 데 반드시 요구되는 공권력 행사를 담당하고 있어 적극적인 참여가 필요한데 소극적으로 참여하거나 공항의 보안조직과 긴밀한 협조를 하지 않으면서 독자적인 업무 집행을 수행하여 마찰이 되거나 문제해결에 부적절했던 사례를 남기고 있다. 예를 들면 보안검색지역에서 항공여객과 검색원 간에 분쟁이 발생했을 때라든지 보안구역 출입시 절차 준수라든지의 문제를 듣고 있다.

② 보안제도 시행상의 문제점

가. 화물 보안의 문제

우리나라 항공안전 및 보안에 관한 법률 시행령에 의하면 여객기 벨리에 탑재할 모든 항공 화물에 대하여 항공사가 공항에서 보안 검색을 실시하도록 되어 있다(안전보안법 시행령 제12조). 이것은 공항에서의 항공화물 처리 지연의

원인이 될 수 있으며 항공화물의 성격상 검색에 의해서 폭약 등의 위험물질을 완전하게 탐지한다는 것이 거의 불가능하여 보안의 효과성도 높지 못하다.

항공화물은 다양한 부피·무게·특성 등으로 검색이 어렵기 때문에 만약 테러리스트의 입장에서 본다면 항공화물을 이용한 파괴행위 기도는 적은 위험부담으로 세인의 관심을 끌 수 있는 좋은 기회가 될 수도 있고, 항공화물에 대한 보안조치는 여객운송에 비해 후 순위이기 때문에 테러리스트들은 이 점을 노리고 항공화물을 이용한 항공테러를 기도할 가능성이 많아 여러 국제기구 및 단체에 의하여 항공화물 보안조치 강화의 필요성과 중요성이 계속 지적되고 있다.

통계에 의하면 2001년 전체 항공사(IATA 회원 가입 항공사)가 정기항공운송을 통하여 운송한 항공화물의 규모는 약 2,800만 톤이었으며, 이 중 여객기를 통하여 운송된 항공화물의 물량은 약 50%에 해당한다. 이렇게 많은 양의 화물을 보안을 위하여 전부 검사한다는 것은 인력과 장비, 각 국가의 개발 정도를 감안한다면 실제적으로 어려운 일이다.

국제민간항공기구가 발간한 항공화물보안 훈련교재에 의하면 항공화물은 검색효과가 적어서 화물을 생성하는 단계에서 보안조치를 취하는 것이 탑재 직전에 검색을 실시하는 것보다 효과적인 것으로 지적하고 있다. 즉, 화주가 화물을 포장하는 단계에서 보안 조치를 취함으로써 불법물질의 내포를 방지하고 지상운송이나 저장 중의 보안 대책도 수립 실천함으로써 공항에서 검색을 실시하는 방법을 지양해야 한다는 것이다. 물론, 화주가 실시해야 할 보안 대책은 현장의 상황을 반영하여 다양한 방법으로 수행될 수도 있으나 그 효과성은 정부가 따져볼 필요가 있는 것이다.

현재 항공화물 보안대책은 국제항공보안의 가장 취약한 분야로 지적되고 있다(ICAO 2000a, Goh 2003). 이는 위에서 지적한대로 항공화물은 공항에서의 100% 검색이 불가능하고 현실적으로 효과적인 보안 대책을 수행하고 있지 못하기 때문이다.

나. 상용화주 문제

항공화물은 공항에서 검색을 사실상 진행할 수 없다는 단점을 보완하기 위해 미국에서는 승인된 특정화주에 대해 공항당국 및 항공사의 검색을 면해주는 제도이다. 즉 승인된 특정화주의 화물은 공항에서 별도의 검색이 없이 선적을 할 수 있도록 함으로서 검색에 따른 적체현상과 비용을 줄일 수 있다.

이를 위해서는 화주기업이 정부가 정하는 기준에 맞는 제도를 마련하고 인력과 장비를 구비해야 한다. 그러나 우리나라의 경우 상용화주제도가 아직 활성화되지 못하고 있다.¹⁰²⁾ 즉 이와 같은 인력과 장비를 갖추고 제도를 운영하는 업체가 거의 없다는 것이다.

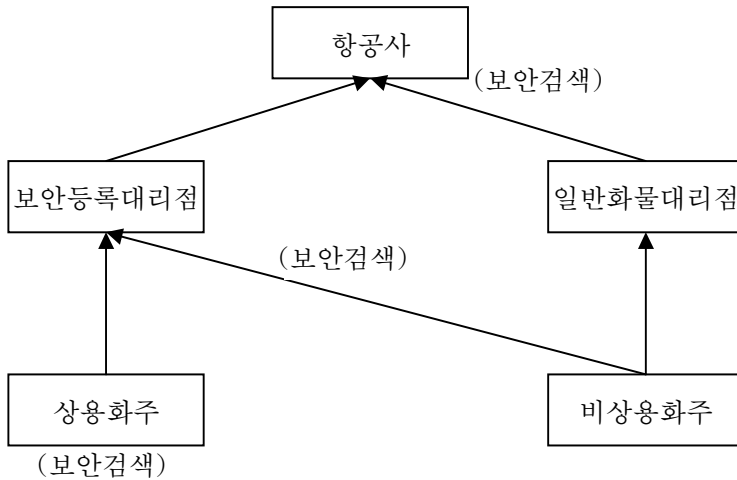
상용화주 인증은 정부에서 결정한다. 그리고 정부가 인증한 상용화주의 화물에 대해서는 항공사에서 신뢰하고 그대로 선적해야 한다. 그러나 우리나라에서 현실적으로 항공사가 이를 그대로 수용할 수 없다. 상용화주로 거론되는 기업들이 사실상 제도, 장비, 인력을 갖추지 못한 상태이기 때문이다. 만약 이로 인해 항공 수송과정에서 사고가 발생시 책임문제는 두고라도 항공사의 이미지와 대외 신뢰도 손실, 경제적 손실문제, 인력손실 등 실제 손실은 항공사가 부담하기 때문이다.

한편, 선진국 중에서도 특히 항공보안에 앞서 있는 미국의 TSA나 EU의 항공기구인 ECAC(European Civil Aviation Conference)도 공항에서의 항공화물 검색의 어려움을 인정하고 보안등록대리점제도(Regulated Agent)를 시행하기로 했다. 이 제도는 항공화물 대리점이 정부 규정대로 보안 대책을 수행하여 공항에 인도한 화물에 대해서는 공항에서의 보안검색을 생략할 수 있도록 하는 제도이다. 또한, 이들 선진 국가들은 화주가 보안대책을 실천하여 화물 운송시스템에 인도한 경우에도 보안 검색을 생략할 수 있도록 하는 상용화주(Known Consignor)제도도 병행운영하고 있다.

102) 건설교통부는 2006년 12월 29일 항공화물을 취급하고 있는 삼성전자 로지텍(주)에 대해 우리나라에서는 처음으로 상용화주 자격을 부여했음.

결국, 항공화물의 보안 검색은 항공화물 물류 흐름의 효율성과 보안 대책의 효과성을 고려하여 다음 <그림 6-1>과 같은 시스템으로 수행되는 것이 바람직하다.

<그림 6-1> 항공화물 보안시스템에서 보안검색시점



즉, 상용화주는 포장, 운반, 저장 단계에서 보안 대책을 수행하므로 상용화주로부터 접수한 화물은 더 이상의 보안 검색의 필요성이 없이 보안등록대리점을 경유하여 항공사로 인도되고, 공항에서도 보안 검색을 하지 않고 항공기에 탑재한다. 또한 상용화주로부터 발생하는 화물은 반드시 보안등록대리점을 경유하게 되는데, 이는 보안등록 대리점이 상용화주를 관리하기 때문이다. 비상용화주로부터 발생하는 항공화물은 보안등록대리점을 경유하는 경우에는 보안등록대리점에서 보안 검색을 하고 공항에서는 더 이상의 보안 검색을 할 필요가 없으며, 보안등록대리점이 아닌 일반 화물대리점을 경유하는 경우에는 공항에서 해당 항공사가 보안검색을 하여야 한다. 이렇게 되면 공항에서의 보안 검색은 비 상용화주가 보안등록화물대리점이 아닌 일반화물대리점을 경유하여 위탁한 화물만 하게 되어 지연이 최소화되고 보안 효과는 최대로 유지할 수

있는 것이다.

다. 외국 항공사의 보안검색 능력 문제

현재 국적 항공사는 인력, 장비 등을 갖추고 있어 제도와 기준에 따라 보안검사가 가능하다. 그러나 한국 공항으로 들어오는 45개의 외국적 항공사의 경우 인력, 장비 모든 부분에서 사실상 검색이 불가능한 상태이다. 외국적 항공사는 우리나라에 보안인력을 별도로 배치하지 않고, 대부분 위탁하여 운영하거나 제도 기준에 미달한 상태로 운영을 하고 있다. 이와 같은 현실은 외국 항공사가 적절한 보안검색조치를 불가능하게 하고 있다.

한편 이러한 문제는 항공화물 수송시 국내화주들이 국적 항공사보다 검사가 상대적으로 소홀한 외국적 항공사에 화물수송을 선호하는 결과를 초래하기도 한다.

라. 항공사의 보안 비용 및 서비스 문제

안전을 위해 보안을 강화하는 데 반대하는 사람은 없다고 하지만, 보안시스템을 갖추고 제도를 마련하여 인력을 가동하는 데는 상당한 비용이 투자된다. 특히 항공사의 경영환경이 악화되고 있는 상황에서 자국 및 외국 공항까지 보안시스템을 완벽히 가동하기는 사실상 쉽지가 않다. 따라서 보안이 강화될수록 비용의 문제는 끊임없이 발생하는 문제이다.

한편 보안을 강화할수록 항공기 여객 및 화물을 위탁한 고객의 불편은 계속 높아질 수 있다. 따라서 항공사의 입장에서는 비용의 제고와 동시에 고객의 불편이 동시에 올라가는 정책을 지속적으로 추진하기란 여간 어려운 문제가 아니다.

마. 보안검색요원의 근무여건과 이직문제

항공여객에 대한 보안검색은 항공보안의 대표적 업무이다. 항공여객 보안검색에 대해서는 현재 공항이 책임을 지고 검색 전문 업체가 서비스를 제공하고 있다. 검색요원들은 소속이 민간회사이면서 업무 과정에서 신체에 대한 검사나

휴대품 검사 등을 수행해야 하는 경우가 많아 피 검색자와 분쟁이 발생하는 경우가 허다하다. 이때 공권력이 없는 신분으로서 저항하는 대상에 대해 직접적 조치를 취할 수도 없고 해당 지역에서 근무 중인 경찰이 신속하게 적절한 조치를 취해주지 않으면 업무 수행이 어렵게 된다. 또한, 우리의 문화가 종적인 관계로 형성된 측면이 많아 고령자나 신분이 높은 사람들은 검색 요원들을 인격적으로 모욕하는 경우도 자주 있는 것으로 파악된다.

검색 요원의 임금수준¹⁰³⁾과 처우도 문제가 되고 있다. 인천국제공항과 같이 여객 처리량이 많은 경우는 또한, 피크 타임에 중단없이 여러 시간 동안 업무를 수행해야 한다는 것도 어려운 점으로 부각되고 있다. 검색 요원의 임금 수준이 낮은 것도 문제로 제기하기도 하나 이보다는 업무의 단순성과 미래에 대한 비전이 열악하여 이직률이 높은 점도 문제점으로 지적할 수 있다.

보안경비요원의 높은 이직은 보안업무의 전문성을 떨어뜨리고 생산성이 낮아진다는 문제를 유발한다. 그리고 이직자에 의한 기밀사항의 유출문제도 우려가 된다. 보안요원은 일반인보다 공항 경비시스템, 보안업무 흐름 등과 같은 내부 정보를 상당히 가지고 있는데, 이직자들이 업무상 취득한 정보의 누출을 실질적으로 막을 수 있는 방법이 없기 때문이다.

한편 항공 및 공항의 보안이 강화되면서 보안경비요원이 급증했다. 그리고 공항의 보안검색 요원이 되기 위해서 의무적으로 특수경비요원교육을 80시간 이상 이수를 해야 한다(<표 6-5> 참조). 그러나 이들 특수경비원교육이 실제 항공보안업무에는 큰 도움이 되지 않는다는 것이 항공사의 의견이다.

103) 인천국제공항보안검색노동조합에서는 2006년 8월에 전체 조합원 투표를 통해 파업을 결의한 바 있다. 인천국제공항보안검색노동조합은 2006년 4월 설립된 신생 노조로 인천국제공항보안검색노동조합에 소속된 노동자들은 특수경비원으로 여객터미널 등 내곽 경비를 맡고 있다. 보안검색 업무를 주로 맡고 있는 이들의 업무형태는 3조 3교대, 주간에는 10시간(휴게 2시간), 야간에는 14시간(휴게 4시간) 동안 일하고 있으며 별도의 휴일 및 휴가 대신 비번을 사용하는 식이다. 그 당시 특수경비원들이 받는 시급은 3,454원 정도로 알려졌다. 보안뉴스 2006. 8. 22일 기사 참조.

〈표 6-5〉 특수경비원 신입교육의 과목 및 시간

구분 (교육시간)	과 목	시간
이론교육 (15시간)	• 경비업법 및 관련법(청원경찰법 · 경찰관직무집행법)	8
	• 헌법 및 형사법 (인권, 경비관련범죄 및 현행법 체포에 관한 규정을 포함)	4
	• 범죄예방론(신고요령 포함)	3
실무교육	• 정신교육	2
	• 테러대응요령	4
	• 폭발물처리요령	6
	• 화재대처법	3
	• 응급처치법	3
	• 분사기사용법	3
	• 출입통제요령	3
	• 예절교육	2
	• 기계경비 실무	3
	• 정보보호 및 보안업무	6
	• 시설경비요령(야간경비 포함)	4
	• 민방공(화생방 포함)	6
	• 총기조작	3
	• 총검술	5
	• 사격	8
	• 체포 · 호신술	5
	• 관찰 · 기록법	3
기타 (4시간)	• 입교식, 평가, 수료식	4
계		88

자료 : 경비업법 시행규칙(법률 제7671호, 2005.8.4)

③ 테러리스트의 공격성 강화와 보안제도의 국가간 격차문제

가. 테러리스트의 공격성 강화와 대응문제

테러리스트들의 기술과 공격성이 날로 강해지고 있다. 테러리스트들의 공격성은 사건당 사망자 수를 살펴보면 여실히 증명된다. 1970~1979년 사이가 0.725명이고, 1980~1989년까지는 1.15명으로 늘어났다. 1990~1999년의 경우 사건당 사망자 수는 1.23명으로 또 다시 증가추세를 나타냈다. 2000년대에 들어서면서도 이러한 추세는 계속되어 사건당 사망자 수는 1.59명으로 증가했다. 사건당 사망자 수의 증가는 테러리즘의 심각성을 보여주는 단적인 증거이다.¹⁰⁴⁾

그리고 테러리스트들의 공격 전술 역시 변화하고 있다. 테러 조직이 가장 선호하는 전술은 폭탄테러가 압도적이다. 1968년부터 2005년까지 발생한 테러 중에 58%인 1만 4,289건이 폭탄 테러였다. 그 다음으로는 무장 공격(4,387건), 암살(2,264건), 납치 및 유괴(1,823건) 순이다. 폭탄을 이용한 공격이 증가하는 이유는 테러리즘의 무차별성과 깊은 연관성을 가지고 있으며, 폭탄 공격의 경우 예방은 물론 사후 대처도 불가능하다. 아울러 일단 폭탄 공격이 성공적으로 이루어지면 증거 확보상의 어려움으로 인해 그 배후 세력을 밝히는 것조차 어렵다는 것이다.¹⁰⁵⁾

그러나 테러리스트들의 공격성에 비해 보안을 맡고 있는 공항당국이나 항공사의 기술은 대부분 현재수준에 머물고 있다. 즉 테러리스트들의 신기술과 치밀한 계획에 의한 테러 등의 범죄는 날로 새로워지고 있는 반면 이에 대한 대응기술을 사고 이전에 개발하는 것이 쉽지가 않다는 문제가 있다.

한편 테러리스트들의 다양한 전술에도 불구하고 정치적 의지만 있다면 테러리즘의 조기 종결이 가능하다는 교훈을 남긴 모가디슈 구출작전 및 엔테베 구출작전의 사례를 거울삼아 이에 대한 테러에 대한 철저한 준비가 필요하다.

104) 최진태, 「테러리즘의 이론과 실제」, 대영문화사, 2006, p. 42.

105) 최진태, 전계서, 2006, p. 49.

〈표 6-6〉 전술에 따른 테러 현황(1968~2005년)

전술유형	사건	부상자	사망자
무장공격	4,387	11,483	6,838
방화	895	309	377
암살	2,264	1,020	2,862
점거대치/인질	205	2,205	897
폭탄공격	14,289	66,309	17,711
하이재킹	233	376	482
납치 및 유괴	1,823	126	956
기타	164	425	236
비재래식 공격	55	2,440	3,004
미확인	286	218	362
합계	24,601	84,911	33,725

자료 : US National Memorial institute for the Prevention of Terrorism(MIPT), Terrorism Knowledge Base.
; 최진태, 「테러리즘의 이론과 실제」, 대명문화사, 2006, p. 49에서 재인용.

나. 보안수준의 국가간 격차 문제

항공기는 국가 및 도시간을 이동하는 운송수단이다. 따라서 특정 국가에서 테러에 대비한 시스템을 완벽하게 갖추고 있다고 해도 다른 나라로부터 들어오는 항공기로부터의 문제가 발생하는 경우 예방이 쉽지 않다. 외국으로부터 오는 비행기는 자국의 공항 내에 착륙한 후에만 보안 검색이 가능하기 때문이다.

실제로 테러범들은 항공 보안시스템이 우수한 선진국가가 아닌 상대적으로 대테러 능력이 떨어지고, 항공보안체계가 허술한 제3세계 국가에서 항공 테러를 자행하는 수범을 사용하기 시작했다. 특히 아시아 및 아프리카 몇몇 국가의 공항에는 아주 기본적인 보안체계도 갖추어져 있지 않은 것이 사실이다. 이들 국가들도 항공 테러예방을 위한 보안 검색시설의 필요성을 인식하고 항공테러 예방을 위한 보안 검색 시설의 필요성을 인식하고 있지만, 기아에 허덕이는 열악한 경제여건으로 인해 막대한 예산이 필요한 보안시설을 갖추지 못하고 있

는 실정이다.¹⁰⁶⁾

문제는 현실적으로 보안수준이 낮은 국가는 분명히 존재하고 이들 국가에 의한 위협이 다른 국가의 보안에도 영향을 준다는 데 문제가 있다. 또한 국제조약을 수용하지 않았거나 준수하지 않는 국가에 대한 처벌도 현실적으로 쉽지 않다는 문제도 있다.

이와 같은 상황 때문에 항공보안의 국가 간의 협정과 국제적인 규범의 통일적인 적용이 필요하다. 그리고 항공보안 취약 국가에 대한 국제적 지원도 요구된다.

이와는 별도로 테러지원 국가를 이용한 항공기 테러 등의 사건도 국제적인 협력이 중요한 이유이다.

(3) 철도 분야

① 정책, 제도, 조직의 미비

철도에 대한 일반인의 인식은 안전하고 정확한 교통수단이다. 철도가 안전한 것은 자체적인 특성에서 비롯되는 부분도 있지만, 우리나라 철도가 국내철도라는 부분도 크게 기인한다.

이에 따라 정부의 정책 및 제도에서 보안 업무는 안전업무 속에 포함되고 있다. 현재 우리나라는 열차 운항중의 기술적인 문제로 인해 발생할 수 있는 사고에 대해서는 매우 다양하게 대책을 마련하고 있지만, 최근 문제가 되고 있는 폭발물에 의한 테러 등과 같은 인위적인 사고에 대한 대책은 미비한 편이다. 정부의 전담 조직이 없는 것도 같은 맥락에서 비롯된 문제이다.

철도의 보안과 관련된 직접적인 법률은 없고 다만 철도안전법(법률7796호, 2005.12.19개정)에서 ‘철도에서 화재·폭발·열차 탈선 등 비상사태의 발생을 대비하기 위하여’ 비상대응계획을 수립하도록 하고 있다(법 제8조). 그리고 동

106) 최진태, 「테러리즘의 이론과 실제」, 대영문화사, 2006, p. 137.

법에서 ‘철도보호 및 질서유지를 위한 금지행위’를 규정한 48조는 테러를 방지하기 위한 법률조항으로는 부족한 면이 많다.¹⁰⁷⁾

미국의 “2005 국경보안개선법(Transportation Security Improvement Act)”이 항공보안, 철도보안 및 해상보안 등을 함께 다루고 있는 것과는 대조적으로 우리나라에서 보안문제는 수송모드별로 개별 기준에 의해 분리되어 별도로 제도가 운영되고 있다.

한편 정부에서는 스페인 마드리드 열차폭탄 테러 사건 발생시 우리나라도 테러분자들의 잠재적인 공격 목표가 될 수 있다며 한국의 경계 태세의 수위를 높이도록 조치한 바 있다. 2004년 3월 스페인 수도 마드리드에서 200명 이상의 사망자를 낸 열차 폭탄 테러 사건과 관련해 고건 대통령 권한대행은 한국의 보안을 강화하도록 지시했다.

② 보안시설 및 장비 미비

보안문제는 의지, 제도, 정책도 중요하지만 장비와 기술력도 매우 중요하다. 테러기술이 계속적으로 발전하고 그 위력 또한 엄청나기 때문에 테러에 대비한 시설과 장비는 테러예방을 위한 실질적인 대응능력이 된다.

그러나 우리나라 철도역/철도는 외부집단에 의한 폭탄 테러, 방화 등을 방어할 수 있는 통제시스템이 부족하다. 철도 100년의 역사(歷史) 속에서 이런 경우가 거의 없었기 때문이다. 가장 기본적인 승객의 휴대품이나 일반화물을 할

107) 법 48조에서 금지하는 행위는 다음과 같다. 1. 철도시설 또는 철도차량을 손괴하여 철도차량운행에 위협을 발생하게 하는 행위. 2. 철도차량을 향하여 돌 그 밖의 위험한 물건을 던져 철도차량운행에 위협을 발생하게 하는 행위. 3. 궤도의 중심으로부터 양측으로 폭 3미터 이내의 장소에 철도차량의 운행안전에 지장을 초래할 물건을 방치하는 행위. 4. 철도교량 등 건설교통부령이 정하는 구역 또는 시설에 건설교통부령이 정하는 폭발물 또는 인화성이 높은 물건 등을 적치하는 행위. 5. 선로(철도와 교차된 도로를 제외한다) 또는 건설교통부령이 정하는 철도시설안에 철도운영자등의 승낙없이 통행하거나 출입하는 행위. 6. 역 시설 등 공중이 이용하는 철도시설 또는 철도차량안에서 폭언 또는 고성방가 등 소란을 피우는 행위. 7. 철도시설안에 건설교통부령이 정하는 유해물 또는 열차운행에 지장을 줄 수 있는 오물을 버리는 행위. 8. 역시설 또는 철도차량안에서 노숙하는 행위. 9. 열차가 운행중 타고 내리거나 고의적으로 승강용 출입문의 개폐를 방해하여 열차운행에 지장을 초래하는 행위. 10. 그 밖의 철도시설 또는 철도차량에서 공중의 안전을 위하여 질서유지가 필요하다고 인정되어 건설교통부령이 정하는 금지행위

수 있는 시설과 장비가 없다. 중장기적으로 철도 이용자에 대한 통제 시스템을 갖추는 문제를 검토해야 한다.

최근에 철도공사에서 경계 침입을 찾아내고 그 위치를 정확하게 파악해 경보해 주는 외곽감지시스템을 갖추기 위해 고속선 영상감지 장비 제품을 도입하고 있어 철도보안 시스템이 한 단계 업그레이드 될 것으로 기대된다. 즉 금번 영상감지장치 제품의 도입으로 향후 고속선 열차 운행 지역의 주변 경계 보안을 강화해 고속선 운행의 안정성을 한층 강화시킬 수 있을 것이기 때문이다.

한편, 철도 선진국 및 국내에서 1996년 이후 발생한 철도사고 발생 현황을 분석하면 전반적인 운전보안설비 개량, 노후차량 교체, 선로구축물 유지관리 개선 등 철도시설 현대화로 운전사고, 운전 장애 및 사상사고의 발생건수는 세계적으로 지속적인 감소 추세에 있다. 그러나 최근 5년간의 국내 철도사고 발생통계를 살펴보면 운전 장애에 의한 사고 건수는 평균 545.4건으로 가장 크게 나타나 대형철도사고 가능성이 상존하고 있으며, 차량 탈선, 송전 등 전력 관련 고장, 시설 보안장치고장 등 장기 열차지연이나 대형 열차사고를 초래할 수 있는 중요한 운전 장애사고는 크게 감소하지 않고 있다.¹⁰⁸⁾ 이는 철도 안전 분야에 대한 전반적인 검토도 필요하다는 반증이다.

③ 국제적인 연대 체제 미비

철도도 이제 국제 테러에 노출된 다중 이용시설이다. 그리고 우리나라도 이라크 파병 등으로 국제 테러의 대상이 될 수 있음이 오래 전부터 지적되고 있다. 따라서 국제 테러로부터 우리나라 철도 이용자와 시설을 보호하기 위해서는 국제적인 연대가 필요하다. 철도 보안에 대한 국제기구의 권고도 수용하고 선진국의 경험과 사례를 전수받고 대비할 수 있는 시스템 구축이 필요하다. 현재 우리나라에서는 철도 보안에 국제적인 연대 협조체제가 부족하다.

108) http://www.krri.re.kr/weekly/2005_weekly/alongsiderail/20050527/1_750.html 철도기술연구원 홈페이지 자료 참조.

2. 물류보안에 대한 관련기관의 의견

연구진은 이 과제를 수행하면서 한국무역협회와 공동으로 2006년 11월 17일 ‘물류보안 대토론회’를 개최하였다. 이날 토론회에는 우리 연구원 및 해양수산부, 미국 국토안보부 담당관의 주제 발표에 이어 지명 토론 순으로 진행되었다. 지명 토론자로는 우리나라의 물류보안제도 시행에 이해관계가 큰 한국무역협회의 한국선주협회 등에서 참석하였다. 이날 토론회에서 제시된 의견을 정리하면 다음과 같다.

1) 한국 선주협회¹⁰⁹⁾

첫째, 물류 전반을 통합적으로 관리할 수 있는 보안제도를 마련할 필요가 있다. 국제적으로 물류보안제도가 강화되고 있으며, 우리나라도 물류보안 장비 및 기술·제도개발에 힘써야 될 것으로 판단되기 때문이다. 이와 함께 국내 화물의 보안기준을 글로벌 기준(예: 미국의 C-TPAT)에 맞추어 우리나라 수출 화물의 안전에 대한 확신을 심어줄 필요가 있다고 본다.

둘째, 항만보안을 확보하기 위해서는 정부가 현재 추진하고 있는 항만 친수 공간 확보정책은 조정할 필요가 있다. 항만 내 친수 공간 확보 정책은 항만물류보안과 상충되는 부분이 있으므로 해결책을 마련해야 하기 때문이다. 이에 따라 항만의 친수 공간 확보 정책은 보안과 결부하여 재검토되어야 한다. 예컨대 민간인의 항만 내 출입은 보안이 인증된 차량에만 허가하도록 하고, 통제하는 것이 바람직하다.

셋째, 정부가 자체적으로 항만의 물류보안 기준을 강화할 필요가 있다. ISPS Code 도입 시행 이후 선박은 항만국 통제제도(PSC)에 따라 보안이 유지되고 있으나 항만의 경우 의무사항에 대한 강제집행 수단이 없어 규정의 실효성 확

109) 한국선주협회 김영무 상무 발언 요지

보에 한계가 있다는 지적이다. 하역인부(일용직 근로자)의 이동시 보안문제, ODCY 내의 보안 문제, 환적화물(북항↔신항)의 이동시 피더 및 보세운송 보안을 담보할 수 있는 법적 기반이 없는 것이 문제점으로 지적되고 있다.

넷째, 물류관련 부처(건교부, 해양부) 및 CIQ 관련기관 간 물류보안체제 구축을 위한 유기적인 협력 체제를 구축할 필요가 있다. 물류보안은 담보하되 이용자에게 최소한의 비용과 시간이 소요될 수 있는 방안이 강구되어야 하기 때문이다.

다섯째, 화주는 화물에 대한 정보를 선주에 적시에 제공해야 한다. 이는 대미 수출화물의 경우 한·미 사이에 체결한 컨테이너 보안협정(CSI)에 따라 선적하기 24시간 전 수화물내역을 미 세관에 신고해야 되기 때문이다. 이 제도를 이행하기 위해서는 우리나라 관세청에 화물정보(manifest) 정보를 제출해야 하는데, 과거에는 화주가 정보를 늦게 제공하거나 잘못된 정보를 제공함에 따라 선사가 피해를 입는 사례가 종종 발생하였다.

한편, 북한의 핵실험 강행에 따라 국내 물류보안에 미치는 영향도 적지 않을 것이므로 이에 대비할 필요가 있다. 최근 북한이 핵실험을 강행함에 따라 향후 우리나라를 포함한 중국 등에서 미국으로 수출되는 컨테이너화물에 대한 보안 검색이 크게 강화될 것으로 예상되고 있다. 국내 항만의 물류보안기준을 강화해 수출화물에 대한 검색비율을 높이고, 우리나라 수출화물이 안전하다는 확신을 심어줄 필요가 있다고 본다. 특히 북한 핵실험 사태가 장기화될 가능성도 있으므로 우리나라 물류보안기준의 국제화 노력도 시급한 실정이다.

2) 한국 무역협회¹¹⁰⁾

한국무역협회는 현재 국제적으로 물류보안이 강화됨에 따라 우리나라도 이 같은 흐름에 따라야 하는 점에 대해서는 찬성하는 입장이다. 그러나 물류보안 강화 조치가 신속한 화물 흐름과 비용 증대를 초래할 것으로 예상되고 있기

110) 한국무역협회 하주협의회 김길섭 국장 발언 요지

때문에 정부는 관련업체와 단체와의 사전 의견 조율이 필요하다는 점을 강조하였다. 또한 우리나라에서 국내 물류보안 체제를 구축하는 경우 정부 부처간의 중복 투자와 유사한 제도의 이중적인 시행을 방지할 수 있도록 정부 차원에서 통합적인 대책을 마련하고, 관련기관 간 협의체를 운영하는 것이 바람직하다는 견해를 피력하였다.

3) 다른 기관 의견

한편, 우리나라의 보안업무를 담당하는 정부 부처에서도 비슷한 의견을 제시하였다. 이 부처는 물류 보안을 강화하려는 해외의 움직임이 빠르게 진행되고 있어 국내에서도 적극적인 대응책 마련이 필요하다고 전제하고, 생산에서 공급에 이르는 전 과정에 걸쳐 물류 보안에 대한 매뉴얼을 마련해 시행할 필요가 있다고 밝혔다.

이 부처는 2006년 9월에 민·관 합동조사를 실시한 결과, 관련 공무원의 물류 보안에 대한 인식 미흡, 항만을 제외한 나머지 물류 현장 포인트에서 보안 취약, 아웃 바운드 화물에 대한 검사 미흡 등이 우리나라 물류보안의 취약요인으로 분석하였다. 하지만 이 같은 분위기 속에서도 국내 항만은 미국에서 요구하는 보안 수준을 충분히 준수하고 있기 때문에 이러한 점을 외국에 적극 홍보하는 한편, 보안업무 수행 우수업체에 대해 인센티브를 부여할 필요가 있다고 강조하였다.

또한 현재 국제기준에 맞게 보안 시스템을 구축할 계획을 추진하고 있으나 관련 부처가 산재되어 있어 사업 시행에 어려움이 있다고 밝혔다. 따라서 앞으로는 국내 물류보안 체제 구축을 위해 부처별로 개별적으로 접근하는 것보다는 특별작업반(Task Force Team)을 구성, 통합적인 작업이 진행해야 한다는 의견을 제시하였다.

이 밖에 관련업체에서도 다양한 의견을 제시하였다. 특히 삼성물산¹¹¹⁾은 미국

111) 이하는 삼성물산(주) 임종인 부장 발언 요지.

에서 물류보안에 대해 신속하고 치밀하게 진행되고 있으며, 요구하는 수준이 높아 이에 대한 적극적인 대책이 필요하다고 밝혔다. 또한 미국 세관 등에서 요구하는 보안 관련 기준과 규격 등에 대해 정확히 파악하고, 관련 장비나 기기 개발에 있어서도 중복 투자를 막기 위해서는 사전에 업체 선정을 통해 준비하는 것이 바람직하다는 견해를 표시하였다.

3. 물류보안제도 정책방향

1) 물류보안 강화에 따른 대책 수립

현재 세계적으로 도입되고 있는 물류 보안 제도의 뿌리는 미국에 있다. 2001년 9·11 테러 이후 미국에서 각종 물류 보안 조치들을 도입한 이후 다른 나라와 국제기구 등으로 확산되고 있기 때문이다. 이에 따라 많은 물류 보안 전문가들은 9·11 테러 참사 이후 대폭 강화되고 있는 보안제도는 사실상 미국에서 마련한 보안 관리시스템을 전 세계에 구축하는 새로운 형태의 ‘미국식 보안제도의 세계화’로 인식하고 있다. 그 구체적인 근거는 다음과 같다.

〈표 6-7〉 미국 물류보안제도의 글로벌화

구 분	초기단계	성숙단계	최종단계
시행방법	업계의 자발적 참여 유도	법률에 의한 강제 집행	국제협약으로 세계 규범화
시행근거	양자 협약	입법 조치	다자 협약
참여기관	미국 관세청	미국 의회	국제해사기구 및 세계세관기구 등
이행수단	인센티브 제공	처벌 규정 도입	회원국의 의무
시행시기	2001~2002	2002~2004	2004년 이후

자료 : 한국해양수산개발원

세계 44개 항만에서 미국행 컨테이너 화물에 대해서 적용되고 있는 컨테이너 보안 협정(CSI)의 경우, 형식은 국가간 양자협약체결 방식으로 시행되고 있으나, 실상은 미국의 적극적인 권유를 수용한 성격이 짙기 때문이다. 국제해사기구(IMO)가 제정해 2004년 7월 1일부터 국제적으로 시행하고 있는 ISPS 코드 또한 미국의 해운보안법을 확대·개편한 것으로 이해하는 것이 옳다. 이 협약을 제정할 당시 미국과 영국이 작업을 주도하는 한편, 선박 보안계획서의 작성과 이행 등 상당히 많은 부문이 미국 법률의 규정을 원용하였다. IMO에서 2007년부터 모든 선박에 설치할 것을 검토하고 있는 장거리 선박 추적 시스템도 미국 해운보안법에 설치가 의무화된 조항이다.

이 같은 경향은 다른 국제기구의 협약 제정 과정에서도 그대로 나타나고 있다. 세계 세관 기구(WCO)가 2005년 10월에 채택한 ‘물류 보안 강화 및 교역 촉진에 관한 기본 협정’이 대표적인 예라 할 수 있다. 미국은 WCO라는 민간 국제기구가 이 협약을 제정하는 과정에 적극 참여, 자국의 이해를 최대한 반영하였다. 이 협정에 포함되어 있는 기본 원칙은 물론 화물정보의 제공 및 수입국의 요청에 따라 수출국 선적항에서 컨테이너 화물에 대한 검사를 시행하도록 규정한 사항 대부분이 현재 미국에서 시행하고 있는 CSI와 24시간 규칙, 그리고 C-T PAT와 같기 때문이다.

즉, 미국은 자국에서 시행하고 있는 물류보안제도를 국제 협약화 함으로써 동일한 기준을 세계에서 시행하는 효과를 거두고 있다. 특정국가에서 제정한 법률이 자국 내에서 시행되고, 그 효력이 관할권이 미치는 지역으로 한정되고 있는 데 비해 국제 협약은 적용 지역이 우선 넓다. 협약 자체에 특별 규정이 없는 한 가입한 국가에서는 동일한 기준이 그대로 적용되기 때문이다. 따라서 시행에 따른 위력이 상당히 크다. 미국이 국제협약 제정과정에서 주도적으로 참여하고 있는 것은 이 같은 효과도 아울러 겨냥한 것이라 볼 수 있다.

따라서 국제화물 운송에 종사하는 물류 기업이나 외국에 상품을 판매하는 제조기업의 경우 미국뿐만 아니라 국제적으로 시행되고 있는 협약의 내용도 면밀히 살펴 대응하는 지혜도 필요하다. 또한 물류 보안 제도는 미국에 그치지

않고, 세계적으로 거의 동일한 기준이 적용되고 있다는 점에 대해서도 유의할 필요가 있다. 미국식 보안기준의 글로벌화는 결과적으로 물류보안에 관한 국제 기준이 점차 강화되고 있다는 것을 의미한다. 전방위적인 대응자세가 필요한 시점이다.

2) 통합 물류보안 시스템 구축

물류 보안 제도도 진화하고 있다. 보안제도가 도입되기 시작된 2001년 이후 1~2년 동안은 주로 선박과 항만을 중심으로 보안기준이 강화되는 데 그쳤다. 미국의 CSI 제도뿐만 아니라 IMO에서 제정한 ISPS 코드 등의 경우 컨테이너 화물을 운송하는 선박이나 그 같은 화물을 처리하는 항만 시설의 보안을 확보하는 데 초점을 맞추고 있었다. 즉 이 당시 물류 보안은 화물 공급 사슬 가운데, 일정 구간에 대해서만 기능할 뿐 다른 운송 분야와의 연계 등에 대해서는 관심을 소홀히 한 것이 사실이다.

〈그림 6-2〉 물류보안제도 적용 범위



자료 : APEC, Total Supply Chain Security 심포지엄 자료, 2006. 7. 6

그러나 미국이 2002년 4월에 도입한 C-T PAT를 2003년 들어 본격적으로 시행하고, 2003년 멕시코에서 열린 아시아·태평양 경제협력위원회(APEC) 회의에서 STAR로 지칭된 토탈 물류 보안 개념이 처음으로 도입된 이후 양상이 크게 변하고 있다. 항만이나 선박에 치중된 물류 보안이 아니라 그 동안 등한시켰던 물류 전 구간을 통합적인 관점에서 보안을 확보할 필요성이 있다는 점이 강조되었다. 2004년 OECD에서 채택한 ‘전 운송 구간 컨테이너 보안’¹¹²⁾이라는 회원국 이행 문서가 작성된 이후 이 같은 분위기는 더욱 확산되었다.

2006년 6월 싱가포르에서 APEC 주관으로 개최된 ‘Total Supply Chain Security’ 심포지엄은 이 같은 움직임의 결정판이라 할 수 있다. 회의 개최국은 이날 기조연설에서 국가 물류 보안계획을 올해 안에 수립, 시행할 방침이라고 밝혔다. 싱가포르 자야 쿠마르 부수상은 이날 심포지엄에서 현행 화물 공급 사슬의 경우 각각 다른 물류업자와 운송 수단이 개입되어 있어 보안상 취약한 점이 많다고 지적하고, 물류 보안은 항만이나 선박 등 특정 운송구간에 있는 물류기업 1~2개 업체가 감당하기에는 한계가 있다고 강조하였다. 2001년 9·11 테러 이후 많은 나라들이 항만이나 공항 등 기간 시설에 대한 보안조치를 강화했으나 물류 전반의 보안은 앞으로 개선할 여지가 많다는 것이 문제점으로 드러났기 때문이다.

싱가포르 방어·전략 연구소도 컨테이너 화물이 이동하는 데는 적어도 25개 물류관련 기업이 연관되어 있다고 말하고, 지금과 같이 항만이 전 운송 구간의 보안문제를 책임지는 데 어려움이 많다고 호소하였다.

싱가포르가 이와 같이 항만이나 항공 등 화물 수출입 지역 위주로 되어 있는 지금의 물류보안제도를 전면 개편하려는 것은 현행 제도가 갖고 있는 보안상의 공백을 메워주고, 화물 공급망에서 가장 취약한 부문으로 평가되고 있는 ‘화물이 처음으로 컨테이너에 적입될 때’부터 최종 소비자에게 인도될 때까지 완벽한 물류보안 시스템을 구축하려는 것으로 풀이되고 있다.

112) Container Transport security across modes

인근 말레이시아 항만과 환적 화물을 놓고 치열하게 경쟁하고 있는 싱가포르의 경우 2002년에 미국이 도입한 컨테이너 보안협정 제도(CSI)를 세계에서 가장 먼저 시행하는 등 ‘물류보안 선점화(先占化) 전략’을 구사하고 있는데, 싱가포르가 ‘토털 물류보안 확보방안’을 강구하고 나선 것도 이 같은 전략과 무관하지 않은 것으로 보인다. 싱가포르에 앞서 유럽연합은 2006년 2월 항만뿐만 아니라 내륙 운송 부문의 보안제도를 강화하는 새로운 제도를 도입하는 등 전 운송구간으로 물류 보안을 확대하였다. 우리나라도 통합 물류보안 시스템 구축을 서둘러야 한다.

3) 물류보안 기술 및 표준 확보

물류 보안과 관련된 기술이나 국제 표준을 선점하려는 다국적 기업 간의 경쟁도 치열하게 전개되고 있다. 물류보안의 확보 여부가 자국 컨테이너 화물의 신속한 처리뿐만 아니라 환적화물을 유치하는 데 필요한 중요한 변수 중의 하나로 대두됨에 따라 각국마다 이에 필요한 시설과 소프트웨어를 갖추어야 하는 등 보안 시장이 날로 커지고 있기 때문이다.

현재 시행되고 있거나 향후 도입이 예정되어 있는 물류 보안 제도와 관련하여 필요한 시설 및 장비, 그리고 정보통신산업(IT)에 기반을 둔 보안 솔루션은 대략 다음과 같다. 주로 컨테이너 화물에 들어 있는 위험화물을 가려내는 장비와 제조업체 또는 항만 터미널 등 물류 핵심시설에 대한 비 인가자 출입을 통제하는 시스템 등이 주류를 이루고 있다.

먼저 컨테이너 검사와 관련해서는 화물 검색기와 방사능 물질 검색기 등에 관한 기술 및 장비 개발·설치 등을 둘러싼 경쟁이 치열하다. 화물 검색기의 경우 1대당 가격이 40억~50억 달러에 달하는 시장을 미국 샌디에고에 본부를 둔 SAIC와 스미스 디텍션(Smith Detection)사가 양분하고 있다고 해도 과언이 아니다. 전자의 경우 ICIS¹¹³⁾라는 토털 솔루션으로 방사능 물질 탑재 여부까

113) Integrated Container Inspection System.

지 검사할 수 있도록 설계되어 있는 것이 특징이다. 트럭에 적재되어 있는 컨테이너를 시간당 16Km까지 검사할 수 있다. 후자는 이동식 컨테이너 검사 장비로 2005년 기준으로 미국과 CSI 협정을 맺은 항만에 27개 시스템을 판매한 실적이 있다. 향후 기술 개발과 관련해 추가 검토가 필요한 사항은 위험화물을 검사하는 데 X-레이 기술을 이용할지 또는 감마 레이 기술을 이용할지 여부와 검사 정보를 화물 정보와 통합, 관리하는 최적의 정보관리 시스템을 개발하는 것 등이다.

또한 비 인가자 출입 통제와 관련해서는 생체 정보를 기반으로 한 이른바 스마트카드를 도입·보급하는 일이 현안으로 남아 있다. 우리나라의 경우 대부분 항만 시설이 출입증 발급·교환으로 이 업무를 대신하고 있으나 미국의 경우 최근 근로자 등에 대한 신원 조사와 새로운 신분증 발급 제도를 도입했다. 인접국인 캐나다도 이에 따르고 있다. 앞으로 지문과 손금, 홍채 및 얼굴 등이 카드에 삽입되는 이른바 생체 인식 기술 스마트카드 및 관독기가 일체를 이룬 출입 통제 장비가 도입될 예정인데, 이 시장의 규모는 미국을 기준으로 향후 10년 동안 10억 달러 이상으로 추정하고 있다.

한편, 이 같은 움직임과 관련해 최근 두 가지 주요한 변화가 나타나고 있다. 이른바 스마트 컨테이너 관련 기술의 개발과 보급을 주도해온 사비 테크놀로지(Savi Technology)¹¹⁴⁾가 대형 군수업체인 록히드 마틴에 인수되었다는 점과 국제컨테이너 보안 협회가 창설되어 물류 보안에 관한 국제 표준과 기술 개발에 적극 나설 가능성이 커졌다는 점이다.

사비 사는 전자 태그(RFID)에 기반을 둔 화물 추적 시스템을 개발해 운영하고 있는데, 현재 미국 국방부와 북대서양 조약기구(NATO) 뿐만 아니라 영국과 덴마크 등 전 세계 국방 관련 업체에서 주로 군수품을 관리하는데 활용되고 있다. 사비 사는 이 같은 활동과 관련해 주로 화물에 대한 전자 태

114) 사비 사는 HPH와 싱가포르 투자 회사인 테마섹 홀딩스, NOL, APL 및 싱가포르 에어 라인, MOL, 오라클 등 세계 굴지의 물류 회사와 솔루션 업체 등이 투자해 캘리포니아 서니베일에 설립한 민간 기업임할 수 있는 소프트웨어를 개발해 제공하고 있음.

그와 신호 판독기, 중앙 데이터 베이스에 화물 정보를 올릴 수 있는 무선 네트워크 시스템, 그리고 고객에게 컨테이너 상태를 전송소프트웨어를 개발해 제공하고 있다.¹¹⁵⁾ 이 같은 사비 사가 록히드 마틴에 인수됨에 따라 미국에서 이와 유사한 시스템을 개발·기술 승인을 목표로 두고 있는 제너럴 일렉트릭(GE)사가 개발한 ‘SecurityGuard’와의 경쟁이 더욱 치열해 질 것으로 보인다.

특히 국제컨테이너 보안 협회(ICSO)¹¹⁶⁾의 창설로 사비와 GE와의 보안 시스템 개발 및 판매, 국제 표준 경쟁은 더욱 가열될 가능성이 커졌다. 비영리 단체인 이 기구는 앞으로 주로 컨테이너 보안장비와 관련된 시스템을 개발하고 국제 표준을 발표하는 것을 설립 목적으로 설정하고 있다. 그런데 공교롭게도 이 기구의 창설 회원으로 참여하고 있는 업체들이 사비사와 경쟁관계에 있는 GE를 비롯해 그린레인 시스템, 제이피 모건 체이스, 일본의 미츠비시, 지멘스, 그리고 컴퓨터 솔루션 업체인 유니시스 등으로 구성되어 있어 향후 활동 내용에 관심이 집중되고 있다. 물류보안기술을 소유한 업체의 발굴 및 육성과 정보통신산업(IT)에 기반을 둔 보안 솔루션 개발에 대한 정부지원 등 체계적인 물류보안기술 육성방안이 마련되어야 한다.

4) 물류보안의 고도화 · 비즈니스화

선사 및 화주 등에 있어 부담이 되는 물류보안제도를 오히려 항만 경쟁력 향상에 활용하는 사례도 나타나고 있다. 컨테이너 물동량 처리를 놓고 선두 다툼을 벌이고 있는 싱가포르와 홍콩이 특히 그러하다.

115) 2005년에 사비사와 허치슨 포츠 홀딩스(HPH)는 합작으로 ‘사비 정보 서비스’라는 회사를 설립, 공동 네트워크를 통해 화주가 컨테이너 화물을 추적하고 관리할 수 있는 솔루션을 제공하고 있는데, 화주들은 이 같은 서비스를 이용할 때 컨테이너 화물마다 일정한 수수료를 납부하도록 되어 있음.

116) International Container Security Organization.

(1) 싱가포르의 대응전략

세계 물류 허브를 지향하는 싱가포르 항만의 경우 2005년에 컨테이너 물동량 2,319만 TEU를 처리, 세계 최대의 컨테이너 터미널로 등극하였다. 싱가포르의 지난해 2,260만 TEU를 처리한 홍콩 항만과 치열한 순위 경쟁을 벌이고 있으며, 인접국인 말레이시아 항만과도 환적화물 유치를 놓고 심한 경쟁 구도를 형성하고 있다.

특히 싱가포르는 세계 해운 중심 전략을 추진하면서 각종 인센티브 제도를 도입, 글로벌 선사를 유치하는 한편, 항만 및 물류 보안 고도화 정책으로 환적화물을 끌어오고 있다. 싱가포르는 미국의 컨테이너 보안 협정(CSI)을 아시아권에서는 처음으로 2002년 7월 2일부터 시행하는 한편, 민간선사와 IT 업체 등이 중심이 되어 개발한 ‘Smart and Secure Tradelane(SST)¹¹⁷⁾’을 시범 운영하는 등 컨테이너 화물 보안 확보에 적극적이다.

싱가포르의 물류보안제도 특징은 미국이 제안하고 있는 거의 모든 컨테이너 화물 검사 제도를 즉각적으로 수용하여 시행하고 있다는 점이다. 미국 에너지부가 컨테이너에 적재되어 있는 방사능 물질을 확인하기 위해 최근 도입한 이른바 ‘Mega Port Initiative(MPI)’를 2006년 4월부터 9월 말까지 시험 운영한 다음 정밀 평가를 거쳐 10월부터 본격 가동에 들어간다. 또한 싱가포르는 미국 국토안보부가 올해 11월까지 시험 운영하고 있는 ‘Operation Safe Commerce(OSC)’ 3단계 사업을 수행하는 등 항만 보안 고도화에 적극 나서고 있다.¹¹⁸⁾

117) 세계 최대의 항만 운영업체인 허치슨 홀딩스와 싱가포르 PSA, 영국의 P&O Ports(디피 월드에 인수), 미 상원의원(정부), 민간전문기업 등이 2002년 7월 출범시킨 컨테이너 보안제도로, SST는 항만운영자가 미국행 선박에 화물을 적재하기 전에 컨테이너를 모니터링하고, 적절한 보안조치를 시행하는 민간 차원의 자발적인 보안 프로그램임. 이 프로그램은 2002년 9월부터 싱가포르와 홍콩에서 미국 시애틀과 타코마 항만으로 수출되는 컨테이너 화물을 대상으로 시험 가동에 착수했음.

118) OSC는 컨테이너에 화물이 적입되는 초기 단계부터 최종 도착지 항만까지 컨테이너가 운송되는 도중에 부정 개폐(tampering)되는 것을 방지하기 위한 물류보안 프로그램의 하나임.

(2) 홍콩항만의 대응전략

홍콩 또한 싱가포르와 마찬가지로 물류보안 선점화 전략으로 컨테이너 화물을 유치하는 정책을 추진하고 있다. 2005년에 컨테이너 물동량 2,260만 TEU를 처리해 세계 순위 2위로 떨어진 홍콩 항만은 남중국 선전과 광저우 항만 등과 치열한 화물 유치 경쟁에 처해 있는 실정이다. 홍콩 항만은 항만 물류 인프라 향상과 컨테이너 트럭 운송 시스템 개선과 함께 입·출항하는 컨테이너 화물에 대한 완벽한 보안 검사시스템을 구축, 적응함으로써 경쟁에서 앞서 나간다는 전략이다.

특히 홍콩의 경우 올 8월부터 항만 보안료 부과제도를 도입함에 따라 항만에서 처리하는 컨테이너 검사비용이 대폭 높아질 가능성이 커졌다. 컨테이너 처리 물동량을 놓고, 싱가포르 항만과 치열한 순위 경쟁을 벌이고 있고, 남중국 화물을 끌어오기 위해 다양한 인센티브 제도를 도입한 가운데, 자체적으로 물류 보안을 강화해 경쟁력을 확보한다는 전략을 추진하고 있었는데, 연간 수백억 원이 넘는 금액을 항만 보안비용으로 투입할 수 있게 되어 이 전략 추진에 탄력을 받게 됐기 때문이다.

홍콩 항만당국은 다른 나라에서는 보통 2% 이하에 불과한 수출 컨테이너 화물 검사비용을 100%까지 끌어올린다는 목표를 정해 놓고 화물 검사 장비를 시험하고 있었는데, 항만 보안료 징수로 이 같은 계획을 앞당길 수 있게 되었다.

〈표 6-8〉 홍콩항만의 컨 물동량 및 항만 보안료 징수 현황(추정)

컨테이너 처리량(2005)	적재 컨테이너 량	항만 보안료	연간 총 징수 금액
2,260만 TEU	1,224만 TEU	20피트 : 2.6 달러	3,140만 달러
		40피트 : 3.9 달러	

자료 : 홍콩 화주 협회 및 한국해양수산개발원

제7장

결론 및 정책 제언

1. 연구 결론

1) 물류보안의 글로벌화 및 영역 확대

물류보안이 새로운 글로벌 메가 트렌드로 부상하고 있다. 2001년 9·11 테러 이후 미국과 국제기구를 중심으로 다양한 보안조치를 강화하고 있기 때문이다. 특히 최근의 물류보안제도는 특정국가 중심에서 벗어나 글로벌 기준으로 확대되고 있다. 이 같은 상황에서 미국이 2006년 10월 13일 항만보안법(SAFE Port Act)을 제정함에 따라 물류보안제도는 더욱 강화될 것으로 예상되고 있다.¹¹⁹⁾

최근의 물류보안 특징은 주요 국가의 화물 생산지에서 다른 나라 소비지까지 전반적인 물류흐름에 대한 안전성을 확보하는 쪽으로 방향이 모아지고 있다. 2004년 국제해사기구(IMO)가 채택한 국제선박 및 항만시설보안규칙(ISPS Code)이 특정 선박 및 항만 등 일정한 구역을 대상으로 하는 보안제도인 데 비해 미국의 항만보안법은 물류 전구간의 보안 확보에 초점을 맞추고 있다.

유럽연합이나 싱가포르 등도 이 같은 추세에 따르고 있다. 세계세관기구(WCO)가 미국의 CSI와 C-TPAT를 기반으로 ‘Framework’를 작성, 100여개 국가에서 시행하기로 합의함으로써 미국의 제도가 세계 규범으로 확대되고 있

119) 이 부분은 연구진과 해양수산부가 공동으로 작성한 정책 자료를 수정·보완한 것임

다. 이 같은 세계적인 경향은 앞으로 우리나라가 이 부문에 초점을 맞추고 필요한 정책을 개발해야 한다는 점을 의미한다.

우리 원과 한국무역협회가 공동으로 개최한 ‘물류보안 대토론회’에서 한국 선주협회도 같은 의견을 표시하였다. 선주협회는 Supply Chain 전반을 통합적으로 관리할 수 있는 물류보안제도가 필요하다고 강조하고, 국제적으로 물류보안제도가 강화되고 있는 점을 고려, 우리나라도 물류보안 장비 및 기술·제도 개발에 힘써야 한다고 제안하였다. 국내 화물의 보안기준을 글로벌 기준(예: 미국의 C-TPAT)에 맞추어 우리나라 수출화물이 안전하다는 확신을 심어줄 정책을 마련해야 한다.

2) 물류보안에 대한 이해 및 인식 부족

물류보안에 대한 이해도를 높이고, 인식의 폭을 넓히는 것도 중요한 과제로 대두되었다. 우리나라의 물류보안 제도는 해양수산부가 2004년에 IMO의 보안제도를 수용하고, 관세청이 세계세관기구(WCO)의 일부 규정을 도입하는 정도에서 그치고 있다고 해도 과언이 아니다. 선사는 물론 화주 또한 물류보안을 새로운 규제 장벽으로만 인식하고 있는 것도 문제점으로 드러났다.

물류보안 토론회에서 국가정보원은 물류보안 대책을 마련하기 위해 최근 부산항과 광양항을 조사한 결과 일반기업은 물론 지방청에서도 이에 대한 인식이 거의 없는 상태였다고 지적하였다. 부산항과 광양항의 일부 터미널이 항만보안에 대해 거의 형식적으로 대처하고 있는 것과는 달리 전 세계적으로 250여개 터미널을 운영하고 있는 허치슨의 경우 자사 운영항만 중 7개 항만에 대해 우선적으로 물류보안시스템을 구축하고, 시범운영하고 있는 것과는 크게 대조된다.

또한 항만과 공항 등 특정 지점에 대해서는 보안의식이 점차 확산되고 있으나 내륙물류 시스템 전반의 보안에 관해서는 거의 손을 못 대고 있는 것도 문제점으로 지적되었다. 세관을 중심으로 이루어지고 있는 컨테이너 화물에 대한

검사도 수입화물에 대한 검사가 거의 대부분이다. 수출 드라이브 정책을 추진하고 있는 우리나라의 정책 여건상 수출화물에 대한 검사를 강조하지 않았기 때문이다. 미국과 컨테이너 보안협정(CSI)을 체결한 전후로 우리나라 항만에 설치되기 시작한 컨테이너 화물 검색기도 밀수 방지 등 수입화물을 주로 검사하는데 사용하고 있다.

앞으로 물류보안에 대한 정부와 민간 기업의 인식 전환이 필요하다. 우선 기본적으로 물류보안의 중요성에 대한 홍보 전략을 수립, 사회전반에 대한 인식을 제고하는 한편, 물류보안 시스템을 우선 구축한 기업에게는 인센티브를 주는 방안과 생산 공장 등 주요거점에 대한 보안 기준을 설정해야 한다.

3) 정부 관계 부처간 업무 조정 미흡

물류보안에 대한 인식 부족은 관계된 정부 부처 사이의 업무 협조와 조정이 곤란하다는 문제도 야기하고 있다. 최근의 물류보안 흐름이 특정 구간의 보안 확보에서 물류 전 구간으로 확대되고 있는 추세를 제대로 반영하기 못하고 있기 때문이다. 이에 따라 우리나라 물류보안은 통합적인 관점에서 체계적으로 추진되지 못하고, 관련 부처별로 ‘각개 약진’하는 성향이 강하다.

예컨대, 물류보안 인증에 대한 사항은 관세청과 산업자원부의 기술표준원이 각기 추진하고 있다. 관세청은 WCO의 Framework를 수용하여 「공인파트너 관리시스템」을 2007년부터 구축할 예정으로 있고, 산업자원부의 기술표준원은 국제표준기구(ISO)의 물류보안활동 표준인 ISO PAS 28000을 국내 도입하기 위한 작업을 진행하고 있다. 또한 해양수산부가 ISPS Code에 의한 항만시설 및 선박에 대한 보안활동을 수행하고 있으나 육상구간의 물류보안을 책임지는 건설교통부는 적극적으로 나서지 않고 있는 실정이다. 이에 따라 우리나라의 물류보안을 구간마다 단절되어 있다.

기관별로 보유한 보안정보의 교류를 통해 유기적으로 협조하는 것이 무엇보다 중요하다. 통합 물류보안 관점에서 각 부처의 물류보안업무를 조정하고, 항

후 실천방안을 담은 ‘국가 물류보안 기본계획’을 작성할 필요가 있다. 물류보안 업무를 통괄하고, 조정하는 기구를 설치하는 방안도 검토해야 한다.

해양수산부의 보안업무도 각각 나뉘어져 있다. 항만시설에 대한 보안은 항만운영과, 선박에 대한 보안은 안전정책담당관실, 물류에 대한 보안은 동북아기획단에서 수행하고 있다. 이와 같이 업무가 분산되고, 각 부서별로 보안 활동의 주안점이 달라 물류보안 체제의 구축 필요성에 대한 공감대를 형성하기 어려울 뿐만 아니라 실질적인 업무 추진에도 한계가 있다는 분석이다. 이에 따라 물류보안의 중요 요소인 항만내 화물보안과 밀접한 연관이 있는 항만시설의 보안 업무와 물류보안업무를 한 곳에서 종합적으로 추진할 수 있도록 업무를 조정하는 것이 필요하다. 항만운영과에서 물류보안 업무를 수행하거나 동북아 기획단에서 향후 항만시설 보안업무를 추진하는 것이 바람직하다는 의견도 제시되었다.

4) 주요 무역국과의 물류보안협력 필요

현재 강화되고 있는 물류보안은 전방위적이다. 미국의 제도가 세계적으로 확산되고 있고, 국제협약으로 제정된 물류보안 기준이 개별 국가에 수용되어 시행되고 있다. 물류보안업무가 확대 재생산되고 있는 것이 오늘날의 실정이다. 이에 따라 각국은 자국의 제도를 강화하면서 다른 나라와의 협력도 강화하고 있다. 컨테이너 화물의 국제적인 이동으로 야기될 수 있는 대량살상무기(WMD) 등의 밀반입을 막기 위한 자구적인 조치로 이해된다.

WCO가 채택한 Framework는 이 같은 국제 협력의 기본원칙을 정하고 있다. 협약 가입국의 요청에 따라 자국에서 수출하는 컨테이너 화물을 검색해야 하는 한편, 그 화물에 대한 정보를 사전에 제공해야 하기 때문이다. 이 같은 제도가 본격적으로 운영되면, 미국이 도입한 CSI와 C-TPAT가 전 세계에서 통일된 기준에 따라 실시되는 것과 차이가 없다. 물류보안제도가 글로벌화하고 있는 가운데, 우리나라가 다른 나라와 물류 보안협력을 강화해야 하는 이유가

바로 여기에 있다.

한편, 홍콩, 싱가포르 등 물류허브화를 추진하고 있는 항만은 자체적으로 화물의 위험성을 점검하기 위한 시스템을 구축하고, 미국과 컨테이너에 적입된 화물의 방사성 물질 여부를 확인하기 위한 ‘Mega Port Initiative’를 시행하는 등 다양한 사업을 진행하고 있다. 정형화된 항만서비스를 차별화함으로써 인근 항만과의 서비스 경쟁에서 우위를 확보하기 위한 수단으로 물류보안 서비스를 활용하고 있는 대표적인 사례로 평가되고 있다. 미국이 도입한 물류보안제도를 적극적으로 수용함으로써 자국 항만의 경쟁력을 강화하고 있는 것이 홍콩과 싱가포르의 또 다른 성장 전략이다.

우리나라 항만시설의 보안 수준은 인근의 중국, 일본에 비해 경쟁력을 갖추고 있다는 분석이 지배적이다. 다만, 컨테이너 화물에 대한 보안체제가 구축되지 않아 대외 협력사업을 수행하는 경우 필요한 시스템 구축에 비용과 인원의 추가적인 투입이 불가피한 것으로 판단되었다. 또한 우리나라 주도로 해외 협력사업을 시행하기 위한 보안 관련 기술과 아이템도 부족한 것도 문제점으로 대두되고 있다.

우리나라의 물류보안제도를 강화하는 동시에 주요 무역국과의 협력도 강화하는 것이 시급하다. 우리나라 자체적으로 물류보안을 강화하는 경우 절반의 효과 밖에 거둘 수 없으므로 주요 무역국에서 보다 신속한 화물처리가 보장될 수 있는 방안을 모색해야 한다. WCO의 Framework의 이행을 준비하는 한편, 미국과의 MPI 시범 사업을 추진하는 것도 효과적이다. 방사성 탐지기를 일정 기간 무상으로 제공할 것으로 예상되는 미국과의 시범운영사업을 우선 시행하고, 이를 바탕으로 다른 국가로 단계적으로 확대하는 것도 노하우를 축적하는데 도움이 될 것으로 판단된다.

5) 민간 기업의 자발적 참여 방안 마련

대부분의 기업들은 물류보안 활동을 새로운 규제조치로 인식하고 있는 경향

이 강하다. 또한 이에 소요되는 비용을 매물 비용으로 생각하고 있어 화물에 대한 보안활동 수행과 프로그램 참가에 소극적일 가능성이 높은 것으로 지적되었다. 그러나 물류보안서비스를 강화할 필요가 있다는 점에 대해서는 대체적으로 긍정적인 의견을 표시하고 있는 것으로 나타났다.

물류보안 토론회에서 한국무역협회는 “물류보안 강화 조치가 신속한 화물 흐름과 비용 증대를 초래할 것으로 예상되고 있기 때문에 정부는 관련업체와 단체와의 사전 의견 조율이 필요하다”는 의견을 제시하였다. 이에 비해 부산 신한만 주식회사(PNC)와 허치슨 터미널 등 일부 하역업체는 서비스의 차별화를 위해 물류보안 활동 수행에 긍정적인 반응을 보이고 있어 국내 업체 사이에서도 의견이 각각 다르다는 것이 드러났다.

이에 따라 물류보안을 새로운 서비스로 발전시키기 위해서는 국내 기업의 자발적인 참여를 유도할 수 있는 ‘물류보안 인증제도’를 도입하고, 일정한 기준을 확보한 기업에 대해서는 인센티브를 제공하는 방안이 필요하다. 관계기관 간의 협의를 통해 물류보안 서비스에 대한 개념을 정의하고, 하역사의 자발적인 참여를 통해 서비스를 수행한 터미널을 거쳐 운송된 화물에 대해 외국 항만에서 보다 신속하게 처리되도록 외국정부와의 협상을 추진해야 한다. 아울러 해외 물동량을 지속적으로 끌어들이기 위한 다양한 혜택을 개발할 필요가 있다.

한편, 한국무역협회는 국내 물류보안 체제 구축과 고품질 서비스 화 등에 대해서 정부 부처간 중복 투자와 제도의 이중 시행을 방지할 수 있도록 정부차원에서 통합적인 대책을 마련하고 관련기관 간 협의체를 운영하는 것이 바람직하다고 제언하였다.

6) 물류보안시장 선점 및 지원 전략 부족

2001년 9·11 테러는 역설적이기는 하지만, 새로운 비즈니스 모델을 제시하는 계기가 되었다. 각국이 물류보안조치를 강화하고, 이에 소요되는 인적 및 물

적 시스템이 개발되면서 하나의 거대한 ‘물류보안 산업’이 형성되기 시작한 것이다. OECD가 2003년에 예측한 자료에 따르면, 당시 국제해사기구(IMO)에서 도입한 ISPS Code를 이행하는 데 따른 전체 비용이 초기 투자비용으로 40억 달러, 그리고 연간 유지비용으로 10억 달러 이상이 들어가는 것으로 추정되었다.

앞으로 물류보안시장 규모는 더욱 확대될 것으로 보인다. 미국이 항만보안법을 제정하면서 기존의 조치를 더욱 강화하고 있기 때문이다. 앞에서 언급한 ISPS Code는 주로 선박과 항만시설에 대한 보안시설을 갖추고, 운영하는 데 초점을 맞춘 제도인데 비해 미국과 WCO 등에서 마련한 제도는 물류 전구간을 대상으로 하는 특징이 있다. 물류보안이 확대됨에 따라 그 비용도 크게 증가할 것이 분명하다.

물류보안시장에 참여하고 있는 글로벌 기업의 추산에 따르면, 컨테이너 보안 장비(CSDs) 및 컨테이너 검사장비, 전자 태그(RFID) 및 스마트 컨테이너 등 물류보안 시장의 규모는 2010년에 연간 90억 달러에 달할 것으로 예상되고 있다. 국제표준화기구(ISO)가 보안표준의 제정을 추진하고 있는 것과 별도로 미국의 록히드 마틴 그룹과 GE가 포함된 국제컨테이너 보안 협회가 각각 보안기술과 장비에 대한 개발사업을 진행하면서 물류보안 시장을 장악하기 위해 치열하게 경쟁하고 있는 이유가 바로 여기에 있다.¹²⁰⁾

특히 물류보안산업 가운데 컨테이너 보안장치와 스마트 컨테이너 시장은 향후 우리나라의 선도적인 정보산업기술(IT)과 결합할 경우 상당한 부가가치를 창출할 수 있는 매력 있는 차세대 성장산업으로 확대될 가능성도 있다. 그러나 우리나라의 경우 전자태그(RFID) 등 일부기술을 제외하고 대부분의 국내 물류 보안 장비 기술은 세계적인 수준에 상당부분 뒤처져 있고, 국내에서의 경쟁 수준에 머물러 있는 것이 문제점으로 지적되고 있다. 또한 우리나라의 물류보안

120) 삼성물산은 최근 150억 원을 투입, GE의 자회사인 컴머스가드(Commerceguard)의 아시아 판매권을 확보하였으며, 해양수산부는 전자태그(RFID) 테스트, 설치 및 실제 항만에서 적용하기 위한 데이터 처리 등에 대한 표준화 사업을 추진하고 있음(2006년 12월 국제표준화기구(ISO)에 제출 예정).

기술이 단 기간 내에 일정 수준에 이르지 못하는 경우 시장의 확대에 인한 경제적 이득을 보지 못하고, 외국기술에 의존할 수밖에 없는 것도 문제점이다.

따라서 글로벌 기준에 적합한 물류보안기술이나 장비 개발을 촉진하기 위해서는 정부차원에서 연구개발사업(R&D)을 지원하고, 국내 보급과 해외진출을 지원할 수 있는 체제를 마련하는 것이 시급하다. 우리나라 물류보안시장이 빠른 시간 내 성장할 수 있도록 전폭적인 지원이 필요하다.

2. 정책 제언

이 연구에서는 앞에서 언급한 연구 결론을 토대로 다음과 같은 정책제언을 제시하고, 2007년 제2차 연구에서는 정책 제언 사항을 반영한 ‘국가 물류보안 기본계획’과 ‘물류보안시장 선점 및 확보 방안’을 수립하는 데 연구의 초점을 맞출 예정이다.

1) 우리나라 물류보안 체제의 세계화

(1) 국가 물류보안 협의체 구성·운영

전 세계적으로 물류보안이 시급한 과제로 대두됨에 따라 관련 업무를 담당하는 정부 부처(국가정보원, 해양수산부, 외교부, 건설교통부, 관세청 등)를 중심으로 가칭 ‘국가 물류보안 협의체’를 구성·운영한다. 이 기구에서는 국제물류 부문에서 야기될 수 있는 위협요인의 평가, 항만·선박·화물 등 물류 전 구간의 대한 보안활동 조치 및 주요 무역국과의 협력 방안 등에 관한 업무를 통합·조정하는 임무를 수행한다.

이 협의체의 설치근거는 해양수산부에서 현재 입법을 추진하고 있는 가칭 ‘국제 항해선박 및 항만시설의 보안에 관한 법률’에 두되 추가적인 법률 개정

이 필요하므로 당분간 이 법률에 포함되어 있는 ‘선박 및 항만시설 보안위원회’를 구성, 활용하는 방안을 검토한다. 또한 정부의 대책과 함께 민간과 정부 사이의 물류보안에 대한 이해와 인식을 제고하고, 향후 물류보안에 관한 기술 및 장비 개발 등 시장 선점 등에 관한 의견 및 자문 등에 활용하기 위해 민간 전문가와 정부가 중심이 되는 가칭 ‘물류보안 포럼’을 구성하는 것도 바람직하다.

(2) 고성능·최첨단 항만보안 시스템 확보

우리나라 수출입 컨테이너 화물을 주로 처리하는 항만에 우선적으로 보안 시스템을 설치한다. 수출입 물동량이 많은 부산·광양항의 컨테이너 터미널을 대상으로 해양수산부, 관세청, 시설소유자 등 관계자간 협력을 통해 수출·환적 화물에 대한 위험성을 평가·관리할 수 있는 체제를 구축하는 것이 시급하다. 미국의 항만보안법 등에서 요구하는 방사능 탐지기, X-RAY 등 비파괴 검색기와 자동으로 화물의 위험성을 감별할 수 있는 장비의 설치가 핵심이다. 수입화물 검사에 주로 활용되고 있는 관세청의 화물 검색기를 수출화물 검사에도 적극 활용할 필요가 있다.¹²¹⁾

또한 항만에 출입하는 사람에 대한 통제 시스템도 고품질화해야 한다. 이 업무를 추진하는 데는 출입자의 편의성과 보안수준을 동시에 향상시킬 수 있는 체제를 마련하고, 단계적으로 확대하는 것이 부작용을 최소화할 수 있다. 항만별로 한정하여 발급되는 출입증을 전국항만에서 통용될 수 있도록 하고, 컨테이너 트럭 운전자 등 보안 활동이 이루어지지 않는 인원에 대한 수시 출입절차를 개선한다. 전자태그(RFID) 기술을 활용한 출입증을 개발하고, 위험도에 따라 폐쇄회로(CCTV) 등 감시장비와 자동 연동되는 시스템을 개발, 주요 터미널에서 시범운영사업을 실시한 뒤 점차적으로 확대한다.

121) 필요한 경우 컨테이너 화물 검색장비의 도입과 인원을 투입하는 데 항만시설소유자가 추가로 부담하는 비용 일부를 보조하는 방안을 검토할 필요가 있음.

(3) 완벽한 통합 물류보안 시스템 구축

현재의 물류보안제도는 항만이나 선박 등 특정구간에서 벗어나 물류 전구간으로 확대되고 있는 것이 새로운 경향으로 나타나고 있다. 선박의 국적여부와는 관계없이 우리 항만을 이용한 국내외 화주, 포워더 등이 최종 목적지의 항만까지 자신의 화물을 추적·관리할 수 있는 시스템을 마련한다. 해양수산부에서 운영하고 있는 해양안전 종합 정보시스템(GICOMS)과 관련부처의 물류 정보 인프라 및 해외의 전자태그(RFID) 기반시설이나 컨테이너 보안장치(CSDs)를 상호 연계하는 사업도 필요하다. 화주와 선사, 터미널 운행사 등과 공동으로 부산·광양항~미 서부 및 동부 항만(시애틀, LA, 뉴욕-뉴저지 등) 사이의 시범사업을 진행한 후 점진적으로 확대한다. 유럽의 항만과 공동으로 이 같은 시범사업을 시행하는 것도 바람직하다.

즉, 컨테이너 화물이 생산되는 공장에서 내륙 운송과정을 거쳐, 항만에서 화물이 선박에 선적된 다음, 외국의 최종 소비자에 이르는 물류 전구간의 보안을 확보할 수 있는 시범사업을 추진하는 계획을 마련한다.

2) 물류보안의 고도화·고품격 서비스화

(1) 물류보안 인증제도 도입, 활성화

민간 기업의 물류보안제도 참여를 유도하기 위해서는 일정한 동기 부여가 필요하다. 대안의 하나로 항만시설 소유(운영)자의 항만, 화물 등에 대한 자발적인 보안활동 수행 정도에 따라 화물처리 간소화 등 인센티브를 제공해야 한다. 이를 위해 항만시설 보안계획서 승인과 별도로 관세청의 C-APM 참가 또는 ISO PAS 28000에 의한 인증 및 화물에 대한 방사성 검사 등 추가적인 보안 활동 정도에 따라 ‘안전 터미널’의 브랜드를 부여하는 방안을 검토한다.

이와 함께 민간 기업의 물류보안을 통한 기업의 이미지 제고 및 마케팅 활용을 촉진하기 위해 WCO와 ISO 등에서 제정한 ‘물류보안 인증제도’가 우리나라에서 조속히 정착될 수 있도록 한다. 산업자원부와 관세청, 해양수산부 등

관련 정부 부처에서 필요한 기준을 제정해야 한다.

(2) 주요국과 화물 신속통관 협정 체결

물류보안은 상대방이 있는 제도이다. 우리나라가 완벽한 시스템을 구축해도 교역 상대국과 협력 채널이 구축되어 있지 않으면 효과는 반감될 수밖에 없다. 우리나라가 보안수준을 인정한 터미널을 통해 운송된 화물에 대해 주요 무역국에서 통관 등에 있어 보다 신속히 처리될 수 있도록 정부간 협력을 강화해야 하는 이유도 여기가 있다.

우선, 수출비중이 높은 국가를 대상으로 협력 방안을 모색한다. 현재 미국이 자국으로 들어오는 화물의 방사성 물질 검사를 위해 해외 항만에서 시범사업을 추진하고 있다. 미국은 우리나라 외교통상부를 통해 이 같은 시범사업의 참가 여부를 타진한 것으로 알려지고 있다. 이는 자연스럽게 물류협력 외교를 강화할 수 있는 기회로 보이므로 적극적인 참여 방안을 검토해야 한다.

(3) 환적 화물에 대한 보안인증제 도입

물류보안은 우리나라에만 한정된 문제가 아니다. 우리나라 항만을 거쳐 외국으로 들어간 환적 화물에 대해서도 책임을 져야 하는 것이 오늘날의 현실이다. 해외에 위치한 화주, 포워더, 선사 등 항만이용자가 우리나라의 물류보안 서비스를 용이하게 인식할 수 있도록 브랜드화 및 마케팅을 추진한다. 우리나라의 물류보안을 항만 경쟁력 확보 및 환적 화물 유치에 적극적으로 활용하는 전략이다.

아울러, 정부에서 추진하고 있는 포트 얼라이언스(port alliance)¹²²⁾와 연계하여 보안 활동이 비교적 미약한 중국의 중소 항만에서 유입된 화물을 국내 항만에서 위험성을 점검하여 제3국으로 운송해 주는 비즈니스 모델을 개발할 필요도 있다. 다만, 이 같은 사업이 성공하기 위해서는 우리나라 항만의 보안

122) 포트 얼라이언스(port alliance)는 해양수산부가 인근 중소형 항만과 네트워크를 구축하여 물동량을 안정적으로 유치하기 위해 추진하는 사업임.

시스템이 완벽하게 구축되어 있어야 하는 것을 전제로 한다.

3) 물류보안을 새로운 성장동력으로 활용

(1) 물류보안 장비·기술 표준화, 상용화

물류보안시장은 새롭게 떠오르는 산업이다. 향후 성장 가능성도 크다. IT와 첨단기술을 접목하는 경우 고부가가치를 창출할 수 있는 새로운 비즈니스 영역이다. 기술개발 및 판매뿐만 아니라 물류보안 인증, 보안컨설팅 등 여러 분야에 걸쳐 일자리를 창출할 수 있는 수요도 적지 않다.

세계 물류보안시장의 확대를 기회로 활용할 수 있도록 해양수산부에서 추진하고 있는 전자태그(RFID) 기술의 국제 표준화를 조속히 추진하고, 장비·기술 및 터미널 설치 노하우 등을 상품으로 개발한다. 우리나라 기술의 활용도 증진을 위해 글로벌 터미널 운영사인 허치슨에서 채택하고 있는 Savi 테크놀로지 등과의 네트워크 연계 방안도 모색한다.

문제는 현재 글로벌 기업들이 각축을 벌이고 있는 컨테이너보안 장비(CSDs)의 표준에 대한 대응이다. 우리나라는 자체적으로 개발한 기술을 상용화하는 정책을 추진하고 있으나 발 빠른 외국 기업들은 이미 자사 제품의 판매를 확대하고 있다. 시장 선점 전략이 시급한 실정이다.

(2) 물류보안 관련 정보 수집·공유 강화

현재의 물류보안제도는 도입 속도가 무척 빠르다. 기술 및 장비의 개발 속도도 가파르다. 물류보안시장을 먼저 차지하기 위한 경쟁 또한 치열하다. 이와 같은 물류보안 정보를 신속하게 확보, 제공하는 것도 시급한 과제이다. 물류보안 토론회에서 국내 기업 관계자는 “미국은 물류보안에 대해 신속하고 치밀하게 대응하고 있으며, 요구하는 수준이 높아 이에 대한 적극적인 대책이 필요하다”고 강조하고, 미 세관 등에서 요구하는 보안 관련 기준과 규격 등에 대해 정확히 파악하고, 관련 장비나 기기 개발에 있어서도 중복 투자를 막기 위해

장치를 도입하는 것이 바람직하다고 제안하였다.

외국정부, 글로벌 기업 및 국제기구 등의 물류보안 추진사항 등 각종 정보를 수집, 가공, 분석하여 국내 기업, 정부 등 관계자에게 제공하는 시스템을 구축해야 한다. 해양수산부에서 우리나라 물류중심전략 지원을 위해 구축하고 있는 ‘동북아 물류정보 센터(KLIC)¹²³⁾’를 활용하는 방안이나 별도의 조직을 설치하는 방안 등 여러 가지 대안이 있을 수 있다.

(3) 물류보안을 차세대 성장산업으로 육성

물류보안은 그 영역이 매우 넓다. 관련 기술간 시너지 효과를 낼 수 있는 부문이기도 하다. 물류보안 신기술을 패키지로 외국에 판매하는 등 수출전략 상품으로 개발할 여지도 충분하다는 의견이다. 스마트 컨테이너나 컨테이너 화물의 방사성 검색기 등 물류보안 장비 수요가 커지고 있기 때문이다. 물류보안을 새로운 비즈니스로 활용하는 전략을 개발해야 한다.

또한 국내 기업의 기술개발을 촉진하기 위해서는 물류보안 시스템을 구축하는 경우 국내 신기술이 우선적으로 사용될 수 있도록 정책적 배려도 필요하다. 현재 일부 부처에서 요구하는 바와 같이 그 동안의 실적위주로 사업자를 선정하는 경우 국내 기술개발 업체가 설 여지가 없어지게 된다. 실적뿐만 아니라 향후 활용도와 성장 가능성을 고려하는 방향으로 사업자 평가방법을 일부 전환하는 검토 작업도 이루어져야 한다.

이와 함께 물류보안 시스템의 외국 판매도 전략적인 접근이 요구된다. 대안의 하나로 우리나라가 현재 추진하고 있는 외국 항만 개발사업¹²⁴⁾과 항만보안 시스템을 연계하는 방안도 있다. 외국 신 항만의 경우 국제적인 기준에 따라 물류보안 시스템을 구축해야 하므로 건설과 보안시스템 설치를 동시에 하는

123) KLIC(Korea Logistics Information Center)는 국내외 물류정보를 수집하여 정책의사결정지원, 물류지도 및 데이터베이스(DB) 서비스 제공을 주 업무로 하고 있으며, 2007년에 시범운영에 착수할 예정이다.

124) 해양수산부는 금융기법(펀드)을 활용하여 국내 항만하역사가 해외 터미널의 인수, 건설, 합병 등 해외진출을 촉진할 수 있도록 지원하는 사업을 추진하고 있음.

것이 효과적이기 때문이다. 아울러 현지 물류보안 인력에 대한 교육과 컨설팅 사업을 시행하는 경우 물류보안 시장의 비즈니스 규모가 더욱 커질 것으로 판단된다.

참고문헌

〈 해운 · 항만 분야 〉

- 김중의, “국제해상보안규정의 주요내용①”, 「해양한국」, 한국해사문제연구소, 2003. 3.
- 남풍우 · 한상현, “미국 컨테이너보안협정(CSI)의 운용현황과 문제점에 관한 연구”, 「산업경제연구」, 제17권 제6호, 2004년 12월.
- 목진용, “항만시설 경비보안제도의 개선방안”, 「해양수산」, 제251호, 한국해양수산개발원, 2005. 8.
- 박준석, 「뉴테러리즘개론」, 백산출판사, 2006. 2.
- 부산항부두관리공사 · 한국로지스틱스학회, 「항만경비보안세미나」, 2006. 12.
- 15
- 여영무, 「국제 테러리즘 연구 : 고대 로마부터 오사마 빈 라덴까지」, 한국해양전략연구소, 2006.
- 정대율, “2005년 항해안전에 대한 불법 억제협약의 국내대응방안 연구”, 「해사법연구」, 제18권 제1호, 한국해사법학회, 2006. 3.
- 최재선, “미국의 항만보안법 제정 의미와 시사점”, 「KMI 해양수산 현안분석」, 한국해양수산개발원, 2006. 11.
- _____, “선사 및 항만, 보안할증료 부과 늘어난다”, 「해양수산동향」, Vol, 1154, 한국해양수산개발원, 2004. 11. 1.
- _____, “중국의 항만 보안료 부과와 시사점”, 「해양수산동향」, Vol, 1222, 한국해양수산개발원, 2006. 8. 2.
- _____, “유엔 결의(1718호)에 따른 북한 선박 및 화물 검색은 가능한가?”, 「KMI 해양수산 현안분석」, 한국해양수산개발원, 2006. 11.

- _____, “최근의 해사보안 강화 동향과 정책 시사점”, 「KMI 해양수산 현안분석」, 한국해양수산물개발원, 2002. 10.
- _____, “해상안전과 보안 동향 전망”, 「해양한국」, 한국해사문제연구소, 2005. 1.
- _____, “IMO 해사보안협력 시행방안”, 「KMI 해양수산 현안분석」, 한국해양수산물개발원, 2003. 3.
- _____, “ISPS Code(선박 및 항만시설 보안규정)가 왜 문제인가”, 「해양수산 동향」, Vol, 1143, 한국해양수산물개발원, 2004. 5. 3.
- 최진태, 「항공테러리즘의 이론과 실제」, 대영문화사, 2006. 6.
- 한국무역협회 · 한국하주협의회 · 한국해양수산물개발원, 「물류보안 대책 마련을 위한 대토론회」, 2006. 10. 17.
- 한국해양수산물연수원, 「ISPS Code의 국내수용방안 연구」, 해양수산물부, 2006. 7.
- 항공보안교육원, 「제3회 항공보안세미나」, 2006. 11. 30.
- 해양수산물부, 「항만시설보안지침서 개발연구」, 2004. 9.
- APEC, 「Papers for APEC Symposium on Total Supply Chain Security」, 2006. 7.
- DOH, 「The National Strategy of Maritime Security」, 2006. 9
- Global Leaders Institute, 「PorTech Asia 2006」, 2006. 9.
- Kilman, Daniel M, 「Japan's security strategy in the post-9/11 world」, McGraw Hill, 2006.
- OECD, 「Container Transport Security Across Modes」, 2004.
- 海洋政策研究財團 · 國際海事大學運合, 「Maritime Terrorism: Developing Case Studies for Teaching and Analysis」, 2006. 3

〈 항공 · 공항 분야 〉

- 강맹진, “9 · 11 테러 이후 미국의 공항 보안검색과 경찰활동에 관한 연구-한국의 경우와 비교 중심으로”, 「한국공안행정학회지」, 한국공안행정학회

회, 2005.

_____, 「한국의 공항보안에 관한 연구」, 동국대학교 박사학위논문, 2001.

강자영·안재형, “항공위협 의 역사적 고찰과 항공보안 관리 연구”, 「한국항공운항학회지」, 제12권 제2호, 한국항공운항학회, 2004년 9월.

고광남·소대섭, 「항공보안론」, 백산출판사, 2006. 3.

김철환, 「항공안전보안개론」, 大旺社, 2004. 12.

김효준, “항공화물전용기의 보안대책”, 「대테러연구」, 제26집, 경찰청, 2003.

유광의, “국제민간항공협약의 표준과 관행을 고려한 공항보안체계의 문제점 고찰”, 「항공우주법학회지」, 2004. 6.

〈 전자상거래 보안, 컴퓨터 보안 자료 〉

김동근 외, “보안운영체제를 위한 자원관리기법 연구”, 「정보보호학회지」, 정보보호학회, 2005. 4.

정조남 외, “전자무역보안과 전략적 대응방안에 대한 소고”, 「정보처리학회 논문지C」, 제11-C권, 제5호, 정보처리학회, 2004. 10.

국가 물류보안체제 확립방안 연구(I)

2006年 12月 26日 印刷

2006年 12月 28日 發行

編輯兼 李 正 煥
發行人

發行處 韓國海洋水產開發院
서울특별시 서초구 방배3동 1027-4
수암빌딩

전 화 2105-2700 FAX : 2105-2800

등 록 1984년 8월 6일 제16-80호

組版・印刷/서울기획문화사 2272-1533 정가 15,000원

판매 및 보급 : 정부간행물판매센터
Tel : 394-0337, 734-6818