

국가 물류보안체제 확립방안 연구(Ⅱ)

2007. 12

최재선 · 목진용 · 황진희 · 고현정 · 김민수

☐ 보고서 집필 내역

◆ 연구책임자

- 최 재 선 : 제1장~제3장, 제6장

◆ 연구진

- 목 진 용 : 제4장
- 황 진 회 : 제5장
- 고 현 정 : 제5장
- 김 민 수 : 제4장

◆ 외부 집필진

- 이 상 윤 (인하대학교 교수) : 제5장
- 민 정 웅 (인하대학교 교수) : 제5장

☐ 산·학·연·정 연구자문위원

◆ 임 종 완 (삼성물산 부장)

◆ 한 범 수 (이비테크 사장)

◆ 김 길 섭 (한국무역협회 국장)

◆ 주 소 령 (산업자원부 박사)

* 연구자문위원은 산·학·연·정 순임

머 리 말

세계 교역 질서에 새로운 패러다임이 자리 잡고 있습니다. 2001년 9·11 테러 이후 미국과 국제사회가 물류보안을 크게 강화하는 조치를 잇달아 내놓으면서 새롭게 형성된 흐름입니다. 이에 따라 국제간 교역에 있어서 물류보안제도는 매우 중요한 변수로 등장하고 있습니다. 글로벌 물류보안제도가 테러 예방과 화물의 안전성을 확보한다는 취지에서 도입됐음에도 불구하고, 제때 이행하지 못하는 경우 통관과정에서 엄격한 검사는 물론 자칫 잘못하면 선박 운항이 지연되는 등 예기치 않은 손실을 입을 가능성이 있기 때문입니다. 이 같은 점 때문에 일부 전문가들은 물류보안제도가 화물의 안전성 확보라는 순기능보다도 ‘물류장벽’이라는 새로운 부담요인으로 작용할 우려가 있다는 의견도 내놓고 있습니다.

문제는 이 같은 물류보안제도가 최근 들어 더욱 강화되고 있다는 점입니다. 미국의 경우 2006년 8월에 항만보안법(SAFE Port Act)을 제정한 데 이어 일년 만에 다시 9·11 테러 대책 이행법률을 제정, 컨테이너 화물의 100% 사전 검색을 의무화했습니다. 이에 따라 특별한 사정이 없는 한 2012년 7월부터 사전 검색을 받지 못한 컨테이너 화물은 미국으로 수출이 금지되는 등 엄청난 파급효과가 일어날 것으로 예상됩니다. 미국뿐만 아니라 세계관세기구(WCO), 국제표준화기구(ISO) 등에서 제정한 물류보안제도도 확산되고 있습니다. WCO는 2005년에 글로벌 교역을 촉진하고, 화물 안전을 강화하는 기본 협정(SAFE Framework)을 제정했는데, 현재 이 협정을 시행하는 나라가 늘어나고 있습니다. ISO도 올 4월에 컨테이너 화물 전자 봉인장치에 관한 국제표준을 채택하는 등 물류보안 기준을 강화하고 나섰습니다.

이 같은 국제적인 동향에 견주어 봤을 때 우리나라의 물류보안 이행 수준은 중간 정도인 것으로 평가되고 있습니다. 해양수산부·관세청 등 정부 부처를 중심으로 물류보안제도를 도입하기 위해 적극 노력하고 있으나 아직 만족할 만한 수준은 아닌 것으로 평가되고 있습니다. 특히 물류보안을 직접적으로 이행해야 하는 민간 부문의 경우 기업 운영에 따른 부담 등으로 소극적인 자세를 보이고 있는 것도 문제점으로 지적되고 있습니다.

우리 연구원이 2006년부터 국가 물류보안체제 확립방안이라는 연구사업을 진행

하고 있는 것도 정부부문에서 국제적으로 강화되고 있는 물류보안제도를 적절하게 이행하도록 지원하는 한편, 민간부문의 부담을 줄이고, 이를 활용하기 위한 전략을 마련하도록 하는 데 있습니다. 이 연구를 토대로 정부와 기업이 새로운 물류 전략을 세우고, 부담을 최소화하는 동시에 물류보안을 활용한 비즈니스 모델을 개발할 수 있기를 기대합니다.

2007년 12월

한국해양수산개발원
원 장 이 정 환

목 차

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

요 약	iii
-----	-----

제1장 서 론	1
---------	---

1. 연구의 배경과 목적	1
1) 연구 배경과 필요성 / 1	
2) 연구 목적 / 4	
2. 선행연구 내용의 분석	5
1) 1차 년도 연구 내용 / 5	
2) 주요 선행연구 검토 / 6	
3) 물류보안 국제회의 내용 / 8	
3. 연구의 주요 내용과 수행방법	9
1) 연구의 주요 내용 / 9	
2) 연구 방법 및 절차 / 10	

제2장 글로벌 물류보안제도 최근 동향	13
----------------------	----

1. 선박과 항만 보안제도	13
1) IMO ISPS 코드 / 13	
2) 미국의 해운보안법 / 16	
3) 운수근로자 신분증 제도 / 18	
2. 컨테이너화물 검색제도	20
1) 컨테이너 보안 대책(CSI) / 20	
2) 미 항만보안법의 시범 사업 / 20	
3) 수입 컨테이너 100% 검색 의무화 / 22	
4) 화물정보 24시간 전 신고제도 / 23	

3. 물류보안 인증제도	23
1) 물류보안 인증 대상기업 / 24	
2) 인증 요건 및 인증 절차 / 26	
3) 인증 기업에 대한 혜택 / 29	
제3장 우리나라 물류보안제도 현황과 문제점	31
1. 우리나라 물류보안제도 현황	31
1) 해양수산부 / 32	
2) 건설교통부 / 33	
3) 다른 부처 / 36	
2. 우리나라 물류보안제도의 문제점	37
1) 제도적인 문제점과 향후 과제 / 37	
2) 기술적인 문제점과 향후 과제 / 40	
제4장 국가 물류보안체제 확보 방안	43
1. 국가 물류보안체제의 개편	43
1) 국가 물류보안 계획 수립 · 시행 / 44	
2) 물류보안 협력사업 추진 / 47	
2. 물류보안 인프라 구축 및 전문인력 육성	61
1) 물류보안 하드웨어 인프라 구축 / 61	
2) 물류보안 전문인력의 육성방안 / 67	
3. 물류보안 위기관리 및 복구 대책	69
1) 필요성과 외국의 사례 / 69	
2) APEC의 물류보안 사고 사후 대응 체계 / 70	
3) 물류보안 사고 대비 국가긴급계획 / 74	
제5장 물류보안산업 전망 및 육성방안	79
1. 물류보안산업 동향 및 규모	79
1) 물류보안산업의 최근 동향 / 79	

2) 글로벌 물류보안산업 규모 / 83	
3) 물류보안산업의 적용 부문 / 89	
4) 주요 물류보안 기술 발전 및 경쟁력 / 91	
2. 물류보안산업 지원·육성 방안	94
1) 정책 목표와 수단 / 94	
2) 물류보안산업 육성을 위한 산업구조정책 / 96	
3) 물류보안산업 부문별 지원 방안 / 101	
 제6장 결론 및 정책 제언	117
1. 연구 결론	117
1) 물류보안은 글로벌 메가 트렌드 / 117	
2) 주요국, 물류보안제도 더욱 강화 / 117	
3) 물류보안 인증제도 시행 확산 / 119	
4) 글로벌 물류보안 정보 과점화 / 120	
5) 물류보안산업, 새로운 수익모델 / 121	
6) 우리나라 물류보안은 ‘중간단계’ / 121	
2. 정책 제언	123
1) 국가 물류보안계획 수립·시행 / 123	
2) 물류보안 관련 법률의 개선 / 124	
3) 물류보안 인증제도의 도입 / 126	
4) 완벽한 물류보안 시스템 구축 / 128	
5) 물류보안산업의 육성 및 지원 / 129	
6) 국가경쟁력에 물류보안을 활용 / 130	
7) 물류보안 연구센터 설립·운영 / 131	
8) 민간 부문의 부담완화도 필요 / 132	
3. 정책 추진 일정표(로드맵)	132
 참 고 문 헌	135
부록 : 싱가포르 및 ISO의 물류보안 인증제도	139

표 목 차

<표 2-1> 시범사업 대상 항만	21
<표 2-2> 주요국의 물류보안 인증제도	24
<표 2-3> 물류보안 인증제도 적용 대상	25
<표 2-4> 운송인 물류보안 인증 특별요건(EU)	27
<표 2-5> 물류보안 인증기관	28
<표 2-6> 주요국의 물류보안 인증프로그램	30
<표 3-1> 부처별 주요 물류보안제도 현황	31
<표 3-2> 우리나라 항공보안 관련 법규	34
<표 3-3> 우리나라 항만의 컨테이너 화물 검색기 설치 현황	37
<표 4-1> 각 부처별 물류보안 추진 업무	46
<표 4-2> WCO 세관-민간 협력 주요 내용	53
<표 4-3> 초고속 컨테이너 검색기 특징	62
<표 4-4> 세계 컨테이너 처리량 및 수송량 추이	64
<표 4-5> 시나리오의 내용	72
<표 4-6> 시나리오의 순차도	73
<표 5-1> 전자 봉인관련 표준 문서	82
<표 5-2> 2015년까지의 보안 분야 시장 성장률 전망	84
<표 5-3> 봉인장치 생산기업별 기술보유 현황	91
<표 5-4> RFID를 활용한 전자 봉인장비 생산기업 및 제품	92
<표 5-5> 방사선 탐지 및 내부영상 검색장비 생산기업 및 제품	93
<표 5-6> GE 물류보안 담당사장의 인터뷰 기사	99
<표 5-7> ISO 전자봉인장치 표준화 범위	102
<표 5-8> 국내 물류관련 IT 업계의 물류분야 매출 비중	115
<표 6-1> 정책 제언 사항 추진 로드맵	133

그 립 목 차

<그림 1-1>	물류보안제도 적용 범위 및 확대 동향	3
<그림 1-2>	연구 수행 절차	11
<그림 2-1>	물류보안 인증 절차	26
<그림 2-2>	물류보안 인증에 필요한 최소 기준(EU)	26
<그림 4-1>	중장기 물류보안 정책 추진 로드맵	45
<그림 4-2>	아시아 게이트웨이 구상에서의 부처 협력	50
<그림 4-3>	물류보안 협력 다층적 구조도	59
<그림 4-4>	물류보안 협력 공고화 방안 구조도	61
<그림 4-5>	컨테이너 보안장치(CSD) 로드맵	65
<그림 4-6>	기술부분 투자 활성화 방안	66
<그림 4-7>	TRP 개념도	71
<그림 5-1>	세계 보안산업 시장규모(2005년)	83
<그림 5-2>	전자산업 내 보안 분야의 시장 규모	85
<그림 5-3>	스마트 컨테이너 시장 현황과 전망	88
<그림 5-4>	경제 및 사회정책의 목표-수단 피라미드	94
<그림 5-5>	물류보안산업 육성정책의 목표와 수단	95
<그림 5-6>	감마선을 이용한 이동식 검색기 VACIS	107
<그림 5-7>	X선을 이용한 고정식 검사기 SACIS P7500	107
<그림 5-8>	X선을 이용한 고정식 검사기 HCVS	108
<그림 5-9>	X선을 이용한 이동식 검사기 HCV CAB 2000M	108
<그림 5-10>	차세대 스마트 컨테이너 개발 모형	111

ABSTRACT

A Study on Assuring Korea's Supply Chain Security against the New Trends of Global Security Issues

After the 9/11 terrorist attacks in the United States, security concerns at home and abroad have been steadily growing. In this context, supply chain security is now increasingly recognized as a matter of cooperation among all players in all sectors of transportation and logistics industry across the world. However, such cooperation can be consolidated with an established domestic supply chain security system. The Korea Maritime Institute initiated a two-year project (2006/2007) on this perspective. In the first-year study, we investigated the current supply chain security issues of various nations and international organizations and then identified Korea's relevant security-related challenges. Based on these findings, this year's study focused mainly on providing a national master plan for supply chain security systems including detailed action plans.

The contents of this second year's study consist of five major chapters : Chapter 1 provides an overview of the objectives of the study and research methodologies. Chapter 2 addresses the recent trend of global total supply chain security (TSCS). Chapter 3 discusses the current situation and problems of supply chain security institutions in Korea. Chapter 4 also suggests ways to secure nationwide total supply chain security. Finally, chapter 5 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, led by the United States, total supply chain security is being established as a global trend. Second, keeping pace with a global trend, a growing number of nations are phasing in a TCSC regime and intensifying it. Third, it is widespread for nations to introduce security validation systems such as C-T PAT and AEO. In

particular, based on its domestic system, each nation is expanding into mutual assurance systems among nations as a tool of cooperation. Fourth, it is increasingly common for nations to have an initiative in the information market on supply chain security. In this global competition, the United States stands out among nations, coming up with brand-new systems such as the “10+2 rule” and GTX (global trade exchange). Fifth, in the process of consolidation of the international TCSC regime, supply chain security industries have newly emerged and are now becoming massive. Global corporations such as GE and Savi are in stiff competition for lion’s share. Last but not least, as for Korea, it has a long way to go in preparing the best practices in its supply chain security regime. Both public and private participants are trying to keep pace with international trends. However, on a mid-to long-term basis, comprehensive solutions and business models should be developed to ensure the best practices.

In addition, the following six major political suggestions in this study are made: Firstly, establishing a national supply chain security plan is necessary. The plan should include the following: 1) basic principles, 2) mid-and long-term policies, 3) policies of each government agency, 4) ways to build infrastructure and to train experts, 5) financial support for R&D, 6) policies encouraging security industries, 7) initiating trade recovery programs after unexpected events such as terrorist attacks, 8) policy on international cooperation. Secondly, an effective legal system should be established. For this, there can be two possible alternatives, namely to revise already-made laws and to adopt new law ruling total supply chain security. Third, the introduction of a validation system for supply chain security should be seriously considered. Fourth, there is an urgent need to establish and operate a completely harmonized supply chain security system. Fifth, it is necessary to develop strategies of supporting and nurturing industries related to supply chain security. Finally, it is important to consider supply chain security as a national economic growth engine and to take advantage of it as a way of beefing up national competitiveness.

요약

제1장 서론

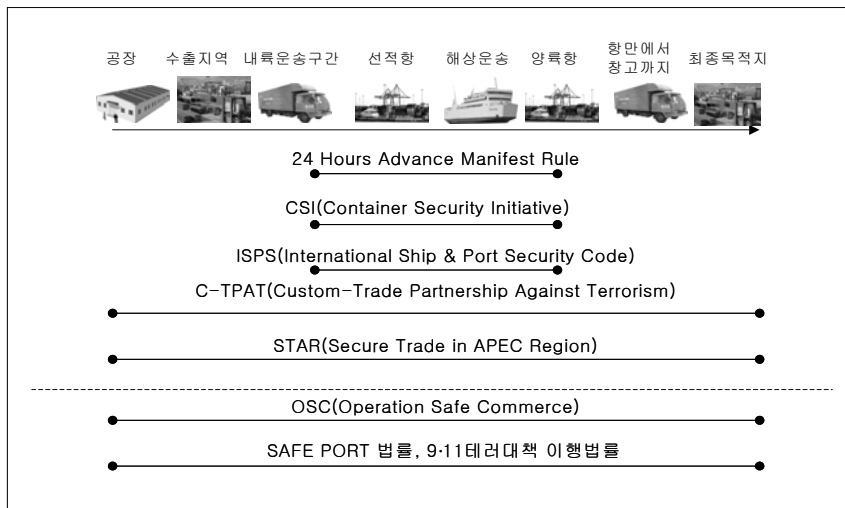
1. 연구의 배경과 목적

- 2001년 9·11 테러 이후 물류보안(supply chain security)이 글로벌 트렌드로 정착
 - 미국 : 해운 보안법 및 항만 보안법 제정 이후 컨테이너 화물 100% 검색 제도 도입
 - 유럽 : 기존 물류보안제도를 강화하면서 기업 물류보안 인증제도(AEO) 시행 예정
 - 싱가포르 : 2007년 5월 아시아권에서는 처음으로 ‘안전한 교역 프로그램(STP) 도입
 - 중국 : 유럽연합(EU)과 미국의 항만을 대상으로 컨테이너 화물추적 시범사업 착수
 - 뉴질랜드 : 세계세관기구의 SAFE Framework를 기초로 미국과 물류보안 협정 체결
 - 국제기구 : IMO와 WCO, 그리고 국제표준기구(ISO) 등 물류보안 강화에 각각 동참
 - ※ ISO는 컨테이너 전자 봉인 장치(E-seal)에 관한 국제 표준을 최근에 확정(2007. 4. 9)
- 국제적인 추세와 우리나라의 현실을 반영한 물류보안제도 도입이 시급한 실정임
 - 외국 물류보안제도가 요구하는 사항에 대한 파악 및 각국의 대응방안 조사 및 분석
 - 우리나라 물류보안제도 미비점을 토대로 향후 정책적으로 활용 가능한 대안을 마련

- 정부 및 민간 기업이 물류보안을 활용해 비즈니스 모델을 개발할 수 있는 방향제시
- 특히 물류보안에 대한 글로벌 동향과 정보를 정부와 기업, 전문 연구가들에게 제공할 필요성도 큰 실정임
 - 9·11 테러 이후 국제적으로 상당한 물류보안제도와 기술이 도입되고 있어 올바른 정보제공이 필요함
 - 또한 이 연구는 정부정책뿐만 아니라 기업의 대응전략 마련에 필요한 ‘정책과 산업’ 부문의 대안을 제시하고 있어 향후 활용가능성과 연구의 독창정도 확보도 고려하였음

<요약 그림-1>

각국의 주요 물류보안제도



2. 선행연구 내용의 분석

- 2006년 수행된 제1차 연구는 주로 테러리즘에 대한 원인 분석과 테러가 발생하는 경우 물류부문에 미치는 영향 등을 분석했음
- 또한 9·11 테러 이후 국제사회에서 도입되고 있는 여러 가지 보안제도 등에 대해서도 심층적으로 검토했으며, 우리나라의 기존 보안제도와 물류보

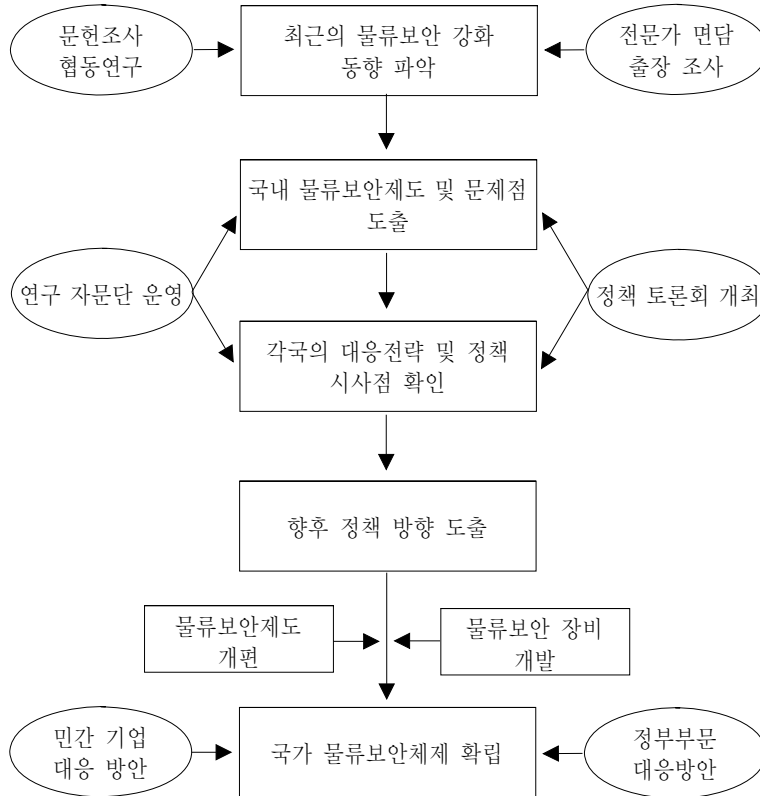
안제도와의 차이점 등도 살펴보았음

- 그리고 이 같은 기본 방향에 따라 앞으로 우리나라는 다음과 같은 세 가지들에서 물류보안정책을 추진하는 것이 바람직하다고 제시했음
 - 첫째, 우리나라 물류보안체제를 세계화하는 것이 시급한데, 그 대안으로, 1) 국가 물류보안 협의체 구성·운영, 2) 고성능·최첨단 항만보안 시스템 확보, 3) 완벽한 통합 물류보안 시스템을 구축해야 함
 - 둘째, 물류보안의 고도화·고품격 서비스화로 우리나라 항만 및 물류 경쟁력을 확보해야 하는데, 그 대안으로 1) 물류보안 인증제도 도입, 2) 주요국과 화물 신속통관 협정 체결, 3) 환적 화물에 대한 보안인증제 도입 등을 제안하였음
 - 마지막으로, 물류보안을 새로운 성장 동력으로 활용하는 전략을 개발해야 하는데, 그 대안으로 1) 물류보안 장비·기술을 표준화하고, 2) 물류보안 정보 수집 및 활용 능력을 제고하는 것이 시급하다고 강조했음
- 제2차년도 연구는 이 같은 사항을 보다 구체화할 수 있도록 국가물류보안 계획(안)을 제시하고, 물류보안산업을 육성·지원하는 데 역점을 두었음

3. 연구의 주요 내용과 수행방법

- 물류보안에 관한 다양한 의견을 수렴하기 위해 협동 연구 및 자문단 구성 운영
 - 우리 원에서 수행하기 힘든 일부 물류보안 기술 및 개발 분야는 협동 연구로 수행
 - 국정원이 주관하는 ‘물류보안체제 구축 민·관 협의회’와 연구 내용 공유 및 협력
- 또한 연구진들은 이 연구를 수행하면서 물류보안 전문가를 대상으로 여러 차례 면담조사를 실시하는 한편, 국제세미나 등에 참여, 글로벌 물류보안 동향을 입수·분석하였음
 - 중국·일본·유럽지역을 방문 항만·물류보안 실태를 파악 및 전문가 면담조사 실시

- 상하이·두바이 등에서 개최된 국제 물류보안 심포지엄에 참석, 전문가들과 의견 교환 및 자료입수·활용



제2장 글로벌 물류보안제도 최근 동향

1. 선박과 항만 보안제도

- 현재 국제적으로 강화되고 있는 물류보안 동향과 특징을 1) 선박과 항만보안제도, 2) 컨테이너 화물 검색제도, 3) 물류보안 인증제도, 그리고 4) 물류보안 기술 부문으로 구분하여 검토하면 다음과 같음

- 선박과 항만의 보안제도는 IMO의 ISPS 코드¹⁾와 미국의 해운보안법, 운수근로자 신분증 발급제도 등이 주축을 이루고 있음
 - IMO는 ISPS 코드를 개정해 2008년부터 선박에 장거리 선박 위치추적 시스템 설치 의무화 및 500톤 이하 선박까지 적용을 확대하는 방안을 검토
 - 미국은 해운보안법에 따라 외국 항만의 보안상태에 대한 평가를 지속적으로 수행 예정
 - 또한 미국은 2007년 10월 1일부터 단계적으로 200만 운수근로자에 대한 신원조회 및 신분증 발급 착수
 - ※ 미국의 운수근로자 신분증 발급제도는 신원조사(background check)와 지문 확보가 주목적

2. 컨테이너화물 검색제도

- 미국이 도입한 컨테이너 보안 협정(CSI)과 컨테이너 100% 검색 시범사업, 그리고 8월 3일에 입법화된 컨테이너 화물 100% 검색 의무화가 주요 내용임
 - 미국은 2002년에 CSI를 도입한 이후 MI(대형항만 방사능 탐지제도)로 검색 기능을 확대·운영
 - 또한 미국은 항만보안법에 따라 컨테이너 100% 검색 시범사업(SFI)을 2007년 3월부터 착수하고, 항만별로 단계적으로 운영에 들어갔음
 - ※ 시범사업에서는 컨테이너 번호 인식기(OCR), 방사능 탐지기, 화물 검색기 통합 설치·운영
 - 미국 의회는 9·11테러 대책 이행법률을 제정하고, 2012년 7월부터 미국행 컨테이너 화물에 대한 100% 검색을 의무화했음
 - ※ 이 같은 법률 제정에 대해 미국뿐만 아니라 세계 선사 및 화주들이 강력하게 반발하고 있음

1) International Ship and Port Facility Security Code : 국제선박 및 항만시설 보안규칙으로 2004년 7월부터 국제적으로 시행되고 있음.

<요약 표-1> 미국 항만보안법에 따른 100% 사전 검색 시범사업 대상 항만

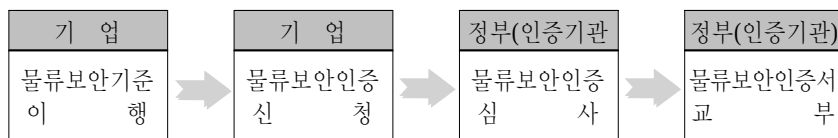
항만	부산항 감만 터미널	카심	사우스 햄튼	싱가포르	살라라	푸에르토 코르테스	홍콩 모던 터미널
국가	한국	파키스탄	영국	싱가포르	오만	온두라스	홍콩
운영	허치슨	디피 월드	디피월드	PSA	APM	Empresa Nacional Portuaria	MT

3. 물류보안 인증제도

- 미국의 반테러 민관협력 제도(C-T PAT) 및 WCO의 SAFE Framework 도입 확산 추세
 - 유럽연합은 WCO에 기반을 둔 물류보안 인증 사업자 제도(AEO)를 입법화하고, 2008년부터 본격적으로 시행할 예정
 - 싱가포르와 뉴질랜드도 안전한 교역 프로그램(STP) 등을 제정하고, 국제 교역에 종사하는 화주를 대상으로 물류보안 인증제도 시행
 - 일본은 지난 2월 관세법을 개정하고, 수출입 화주를 대상으로 물류보안 인증사업에 착수한 데 이어 국토교통성도 운송기업에 대한 인증제도 도입 추진
- 한편, 기업이 물류보안 인증을 받기 위해서는 일정한 보안기준을 이행하는 등 인증 기관의 보안심사를 통과해야 하는데 그 절차는 아래와 같음

<요약 그림-2>

물류보안 인증 절차



자료 : 한국해양수산개발원

<요약 표-2>

주요국의 물류보안 인증제도 비교

	미국	EU	WCO	일본
프로그램	C-T PAT	EU 세관법 및 시행규칙	국제무역의 안전확보 및 원활화를 위한 기준(SAFE Framework)	적하, 여객 및 승무원에 관한 사항의 사전보고제도
관할기관	미국 세관(CBP)	EU 가맹국 세관	WCO 가맹국 세관	재무성 관세국
프로그램의 법제화 여부	CBP와 민간 임의 프로그램	2005년 4월13일 개정관세법, 2006년 12월 18일 개정 시행규칙	2005년 6월 23일 WCO총회에서 기준 채택	관세법, 관세법시행령
적용 대상	수입	수입 및 수출	수입 및 수출	수입
대상 기업	미국의 수입자, 캐리어, 포워더, NVOCC, 특정외국 기업, 브로커	AEO(통관에 관련한 업무를 실시하는 물류 부문 중 사기업)	AEO(기업, 수출입자, 운송인, 브로커, 오퍼레이터 등)	선박회사, 항공회사, 혼재업자(예정)
목적	•세관은 모든 수입화물을 검사할 책임이 있음 •C-T PAT는 수입, 수출 등 미국으로의 수입화물에 직접적으로 책임을 부담하고, 법을 준수하는 low-risk 기업의 참가를 요구	•지금까지 개별적으로 간 이통관 절차 허용 •EU 차원에서 제도를 일반화, 보안 필요요건을 지키는 기업에게 AEO 지위 부여	•글로벌 차원에서 물류 안전 확보 및 원활화 •모든 수송수단에 대하여 통합된 SCM을 가능하게 지원	일본의 테러행위와 국제적인 범죄조직을 미연에 방지
요건	•거래처 보안 요건 •보안 절차 등 포함 •내부보안 기준 및 컨테이너보안 등 이행	•적절한 이행 기록 •상업과 수출에 관계된 기록의 관리 •재무적 건전성의 증명 •보안과 안전기준	•세관요건의 준수 •상업기록의 관리 •재무의 건전성 •화물의 보안 등	
혜택	•검사횟수의 감소 •우선적인 검사 시행	•관세규칙에 기반한 통관 간소화 •보안과 안전에 관계된 세관관리의 원활화	•화물의 양도를 촉진하는 수단, 수송시간의 삭감과 보관비용의 저감	
화물 정보의 사전 통지	•해상 컨테이너 화물 수입-외국항에서 선적 24시간 전 - 수출-미국선적항 출항 24시간 전 •항공화물(장거리 비행) 수입-미국도착 4시간 전 - 수출-미국출발 2시간 전	•해상 컨테이너 화물 수입-출발항에서 선적의 24시간 전 - 수출-EU출항본선으로의 선적24시간 전 •항공화물(장거리 비행) 수입-EU도착 4시간 전 - 수출-EU출발 30분전	•해운 컨테이너 화물 출발 항에서 선적 24시간 전 •항공화물(장거리비행) 발송국의 최초 공항으로 도착 4시간 전	•해상컨테이너 화물 입항하기 24시간 전까지 보고 근거리는 입항 12시간 전 또는 입항 전 •항공화물 - 항공시간 5시간 이상-입항 3시간전 3시간 전~5시간 미만-입항 1시간전 3시간 미만-입항하기까지

자료 : 일본 Cargo, 2007년 6월호를 토대로 한국해양수산개발원 재 작성

- 주요국이 물류보안을 강화함에 따라 이에 필요한 물류보안 시장도 점차 커지고 있는 것으로 나타났음
 - 컨테이너 보안 장치(CSD) 및 검색, 전자 태그(RFID) 시장은 2010년에 90억 달러에 이를 전망
- 이에 따라 GE나 록히드 마틴 등 글로벌 기업의 물류보안 시장 참여도 본격화되고 있음
 - 컨테이너 보안 장치(CSD) 및 컨테이너 전자 봉인 시장 : GE와 록히드 마틴이 각축전
 - 컨테이너 화물 검색기 시장 : 스미스 디텍션, 중국의 누크테크, 미국의 SAIC 등 3파전 형성
 - ※ 컨테이너 화물 검색기는 OCR, 방사능 탐지기, 화물 검색기 기능이 통합된 모델이 현재 상용화되고 있는데, 이 같은 통합모델이 주종을 이룰 것으로 전망됨

제3장 우리나라 물류보안제도 현황과 문제점

1. 우리나라 물류보안제도 현황

<요약 표-3>

우리나라 물류보안제도 시행 현황

부처 별	주요 제도
해양수산부	1. ISPS 코드 등 IMO 보안협약 시행 2. ISPS 코드 이행법률 제정(5월 14일) 3. 컨테이너 100% 검색 시범사업 추진(2007년 중)
건설교통부	1. 항공안전 및 보안에 관한 법률 시행 2. 항공 부문의 상용화주제도 도입 3. 내륙 교통부문 보안제도 도입 추진
관 세 청	1. 미국과 컨테이너 보안 협정(CSI) 체결, 시행 2. 유럽연합 일부국가와 화물추적 시범사업 협정 체결 3. 공인 사업자 수출입 안전관리 우수 공인업체 지정 추진
국가정보원	1. 물류보안체제 구축 민관 협의체 구성·운영

자료 : 한국해양수산개발원

- 해양수산부를 중심으로 물류보안을 확보하기 위해 적극 나서고 있으나 아직 중간단계에 불과한 실정임

2. 우리나라 물류보안제도의 문제점

1) 제도적인 문제점과 향후 과제

- 통합 물류보안제도가 정립되어 있지 않음 : 우리나라의 경우 물류 전 구간을 통합·관리하는 완벽한 물류보안체제가 구축되어 있지 않은 실정임
 - 앞으로 물류 전 구간을 완벽하게 통합하는 물류보안제도를 도입하는 것이 필요함
- 물류보안 기준이 마련되어 있지 않음 : 운송인이나 제조업체 등 물류와 관련되어 있는 기업이 준수하고 이행해야 하는 최소한의 보안기준이 마련되어 있지 않음
 - 미국, 유럽연합, 싱가포르 등의 제도를 토대로 각 부문별 물류보안에 관한 최소 기준을 설정하는 것이 시급함
- 기존의 물류보안제도에도 미비점이 있음 : 내륙 및 도로 등에 관한 물류보안제도가 없고, 기존의 ISPS 코드 시행도 형식적이라는 지적이 있음
 - 제도 흡수를 메울 수 있는 대안을 마련하는 한편, 기존 제도 이행을 강화하는 시스템이 필요

2) 기술적인 문제점과 향후 과제

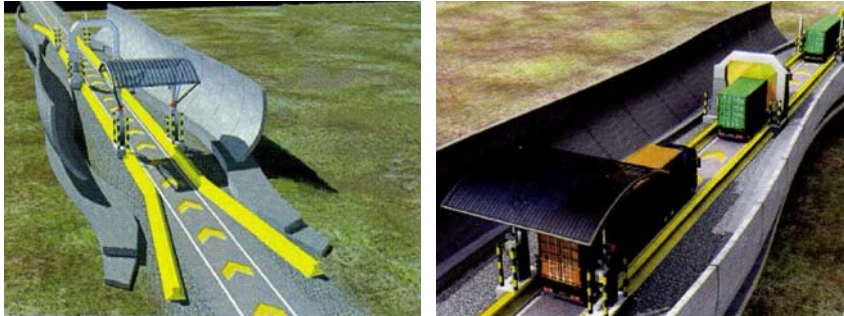
- 물류보안산업의 육성 및 활용전략이 없는 실정임 : 우리나라는 물류보안 확보에 필수적인 기술 및 장비 개발이 이루어지지 않아 향후 선진국에 기술 종속 우려
 - 물류보안 시장이 새로운 성장산업으로 부각되고 있으므로 이를 활용한 기술 개발 및 투자가 이루어져야 함
- 항만 물류보안 시스템이 구축되어 있지 않음 : 우리나라 항만에 수입화물을 주로 검사하는 화물 검색기가 설치되어 있을 뿐 다른 물류보안장비 도

입이 거의 이뤄지지 않은 실정임

- 제품을 생산하는 공장으로부터 중간 운송단계를 거쳐 최종소비자에 이르는 물류 전 구간을 포함한 컨테이너 화물 전자 잠금장치, 화물 추적 장치, 화물 검색 시설 및 물류보안정보를 통합·관리하는 시스템을 구축해야 할 것임

<요약 그림-3>

로테르담 항만의 컨테이너 통합 검색 시스템 개발 모델



자료 : 로테르담 항만청

- 물류보안정보의 통합·관리에 대한 준비가 부족함 : 우리나라의 경우 화물 및 통관 정보 등을 관리하는 싱글 윈도우 시스템을 추진하고 있으나 물류보안 정보와 연계되어 있지 않은 실정
- 국제적으로 물류보안이 강화되면서 화물 및 화주, 선적 정보, 그리고 컨테이너 화물 검색정보제공을 요구하고 있으므로 이에 대한 시스템을 갖추는 것이 필요함

제4장 국가 물류보안체제 확보 방안

1. 국가 물류보안체제의 개편

1) 국가 물류보안 계획 수립·시행

- 국가 물류보안체제를 확보하는 방안의 하나로 제시된 국가 물류보안 계획

기본 방침을 토대로 마련하면 될 것임

- 1) 글로벌 물류보안 강화 추세에 적극 대응하는 물류보안체제 구축, 2) 동북아 인근 항만에 앞서 신속하게 물류보안체제를 구축함으로써 항만 경쟁력 확보 및 차별화된 부가가치 창출, 3) 물류보안정책 협의체를 구성·운영, 4) 물류보안제도를 조기에 정착하기 위해 민간부문의 자발적인 참여유도 방안, 5) 물류보안산업을 육성하고, 비즈니스 모델을 개발하는 등 정책 지원 강화, 6) 물류보안의 국제적 확산에 필요한 대외협력을 강화하는 내용을 반영하도록 했음

<요약 그림-4> 중장기 물류보안 정책 추진 로드맵



- 또한 국가 물류보안 계획에 반영될 우리나라 물류보안 중장기 정책방향은 아래와 같은 일정에 따르도록 했음

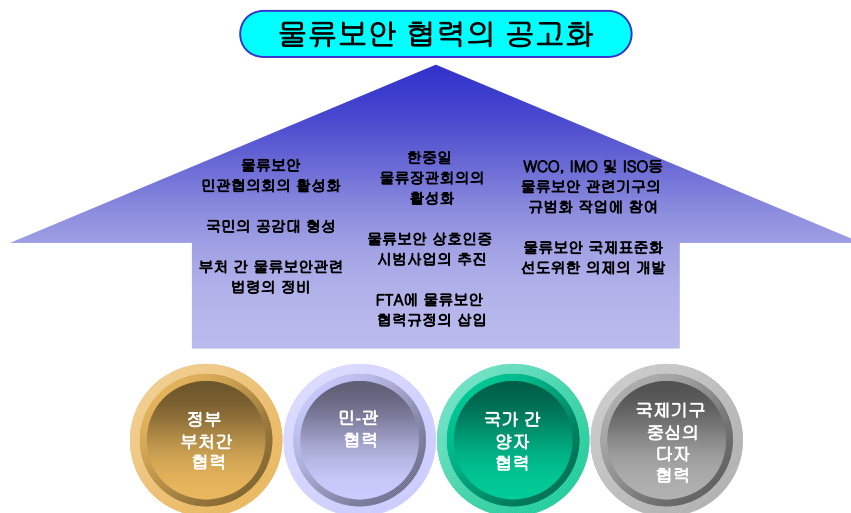
2) 물류보안 협력사업 추진

- 물류보안은 화물과 함께 오는 국가안보 위협에 대응해 국가안보를 확보하는 한편, 글로벌 무역의 원활화를 확보하기 위해 필요한 것으로 국가 간 협력이 전제가 되어야 함

- 이러한 협력은 크게 국내와 국제협력으로 나뉘 볼 수 있으며, 국제협력은 정부간 양자·다자협력과 국제기구에서의 협력으로 나뉘볼 수 있음
- 현재 국제 물류보안 협력은 양자적, 다자적으로 다차원적으로 이뤄지고 있음
 - 정부-정부 차원에서는 미국-캐나다의 FAST, APEC TRP 등이 있음
 - 정부-민간 차원에서는 C-T PAT, AEO제도 등이 있음
 - 민간-민간 차원에서는 ICSO, 기술 분야 민간기업 파트너십 등이 있음
- 우리나라의 경우 국내협력 차원에서는 ‘물류보안 민·관 협의회’가 운영되고 있으나, 비상임이며 비공식기구로의 한계를 가지고 있으며, 물류보안을 전담하거나 협력을 주도하는 기구는 아직 없는 상황임

<요약 그림-5>

물류보안 협력 공고화 방안 구조도



자료 : 한국해양수산개발원

- 국가 간 협력의 경우, 관세청 및 해양수산부를 주도로 하여 AEO 시범사업 및 국제협약의 국내이행법 제정 등을 통해 국제사회의 추세에 어느 정도 따라가고 있음
- 하지만, 물류보안제도 및 인프라를 구축하고 중장기적인 협력과제를 효율적으로 수행하기 위해 필요한 정책은 아직 마련되어 있지 않음
- 따라서 우리나라의 경우도 국내협력을 바탕으로 국제협력을 강화하는 다

차원적 협력체계를 구축하기 위한 정책마련이 필요함

2. 물류보안 인프라 구축 및 전문인력 육성

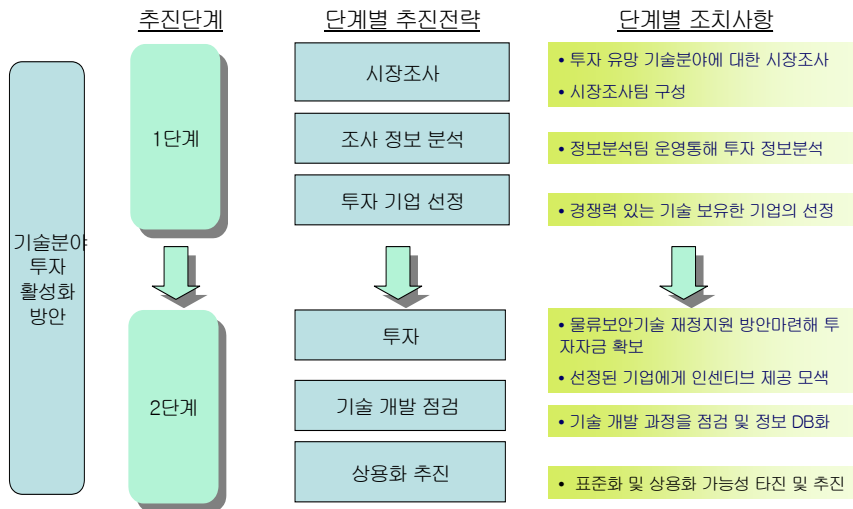
1) 물류보안 하드웨어 인프라 구축

- 현재 물류보안 하드웨어 인프라 시장은 가히 폭발적으로 성장하고 있음
 - 스마트 컨테이너 시장의 경우, 2006년 약 7,000만 달러에서 2012년에는 약 42달러로 비약적인 성장을 보일 것으로 기대됨
 - 한편, 향후 미국의 100% 검색법이 시행되는 경우, 초고속 컨테이너 검색기의 수요 또한 급증할 것으로 전망됨
- 우리나라의 경우, 2006년 기준으로 대미 컨테이너 검색 필요량은 총 140만TEU였으며, 2012년까지 평균 물동량 증가율을 20%로 가정할 경우, 검색이 필요한 컨테이너는 420만개에 이르게 될 것임
 - 이를 필요한 초고속 컨테이너 검색기로 환산할 경우, 필요한 검색시스템의 수는 42대에 이르며, 금액으로는 1조원에 해당됨
 - 따라서 우리나라 물류보안 과제는 인프라 구축을 통해 물류보안이라는 실질적 이득을 취하는 동시에 물류보안 시장경쟁력을 강화하는 것이라고 볼 수 있음
- 이러한 측면에서 물류보안 하드웨어 구축방안 마련은 중요하게 대두되고 있으며, 그 방안으로 크게 인프라 구축에 대한 공감대 형성, 기술연구개발 지원, 기술표준부분 이니셔티브확보 지원 및 기술투자 활성화 방안으로 나뉘어 살펴볼 수 있음
- 인프라 구축에 대한 공감대 형성
 - 정부주도하에 화주를 포함한 참여주체들의 물류보안에 대한 인식이 강화되고, 물류보안을 통한 물류효율성 향상에 대한 공감대가 형성되어야 함
 - 2006년 제1차년도 연구를 시행하는 과정에서 연구진이 수렴한 의견조사에 따르면, 한국선주협회, 한국무역협회 등은 물류보안제도 마련에 원칙적으로 찬성했음

- 다만 제도를 급격하게 도입하는 경우, 관련업계에 미치는 영향이 클 수 있으므로 점진적인 제도 도입을 요청했음
- 기술 연구개발 지원
 - 전자봉인 장치 시장의 경우 모든 컨테이너에 1회성 전자봉인 부착 시 40피트 컨테이너를 기준으로 약 2억 개의 전자봉인이 소모될 것임
 - 스마트 컨테이너 시장의 경우 대규모시장보다는 화학, 군수, 고가귀금속 및 반도체 등 전문화된 시장을 중심으로 확장될 전망이다
 - 이러한 물류보안 하드웨어 시장은 궁극적으로 IT시스템과의 연계가 필수적이라서 IT강국인 우리나라 기업의 경쟁력이 높은 분야임
 - 이를 위해서 기술 개발은 민간기업이 선도하고, 재정적 지원은 정부가 제공하는 민-관 파트너십에 의한 R&D 사업추진이 바람직함
- 기술표준부분 이니셔티브 확보
 - 전자봉인의 경우 국제표준기구를 통해 433MHz와 2.45GHz 주파수를 모두 지원하는 방안이 확정되었음
 - 이와 함께 물류보안산업에서의 기술표준 제정이 지속적으로 이뤄질 것으로 전망되면서 분야 별 표준작업 가능성을 타진하고 우리나라의 입장을 정리하는 작업이 필요함
 - 이를 위해 기술개발 및 연구와 그 결과를 중심으로 한 표준화 작업이 함께 이뤄져야 하며, 이를 통해 국제표준 이니셔티브를 확보할 수 있도록 해야 함
 - 특히 국제표준 가능성이 있는 분야(특히, 스마트 컨테이너 등)를 선별하고, 이러한 분야에 대해 산업자원부의 기술표준원을 중심으로 민간기업과 정부가 공동으로 논의하는 협력창구 마련이 핵심
- 기술부분 투자 활성화 방안
 - 기술 연구 및 개발은 정부의 적극적 지원과 민간기업의 전략적 투자를 바탕으로 함
 - 정부가 물류보안산업을 정책적으로 지원하면서 인프라 구축에 힘쓰는 한편, 기업은 이를 토대로 한 시장경쟁력을 높일 수 있도록 이를 뒷받침할 투자가 활성화되어야 함

<요약 그림-6>

기술부분 투자 활성화 방안



2) 물류보안 전문인력의 육성방안

- 보안인증제도 시행과 이에 필요한 전문 인력의 양성이 필요함
 - 각 업체의 물류보안 위험성을 평가하는 전문가
 - 각 업체가 수립한 보안경영시스템 인증심사 전문가
- 컨테이너 및 항만보안장치의 설치 및 운영관련 전문가 양성 필요함
 - 컨테이너 보안장치 및 데이터 암호화 등 정보기술분야 전문가
 - 컨테이너 검색장치 운영 및 검색(스캔) 내용 판독 전문가
- 보안사고에 대비한 긴급계획 수립이 필요하며, 이를 담당하는 보안책임자 및 보안요원의 양성 및 전문성 제고 필요함
 - 긴급계획 수립 전문가(planner)
 - 현장지휘자(on-scene commander) 및 대응요원

3. 물류보안 위기관리 및 복구 대책

- 물류보안은 크게 사전적 보안과 사후 대응방안으로 나뉘볼 수 있음
 - 현재 물류보안 논의의 주류는 사전적 보안체계 마련에 맞춰져 있으나,

- 테러와 같은 사건 발생 후에 국가 간 협력을 통해 조속히 무역을 재개하는 것을 골자로 하는 사후 대응방안도 APEC 등 국가 간 협력체에서 본격적으로 논의되고 있음
- 국가 간 협력에 앞서 국내차원에서 보안 사고나 사건의 영향을 최소화하기 위한 위기관리 및 복원 절차가 마련되어야 함
 - 이와 관련해 제시된 국가긴급계획에는 1) 계획 수립 및 책임기관 지정, 2) 대응조직의 설립, 3) 정부와 업체의 공조체제 구축, 4) 단계별 대응 매뉴얼 작성, 5) 보안사고 발생 가능구역의 설정 등이 포함될 수 있음
- 이를 위해 APEC의 조속한 무역재개를 위한 프로그램(TRP)이 주는 시사점이 큼
- TRP는 테러가 발생한 이후 신속한 무역재개를 확보하기 위해 필요한 주요 원칙, 범위 및 요건들을 제시한 것임
 - 이 개념에서 강조하는 사항은 국가 간 무역재개 활동들을 조정하며 늦장 대처로 인해 발생하는 손실을 최소화하며 공급 망 보안을 확립하는 것임
 - TRP는 1) 테러사건 발생 직후의 행동계획(Plan of Action), 2) 대응 모범지침(Model Guideline), 3) 회원국간 의사소통(Communication)의 세 가지 내용으로 구성됨
- 한편 국가 물류보안 기본계획의 일환으로 보안 사고나 사건의 영향을 최소화하기 위한 위기관리 및 복원절차가 필요함
- 이러한 대응체계마련의 목표는 화물의 제조에서 최종소비에 이르는 과정에서 발생한 보안사고에 대응하기 위해 공적·사적 자원을 포함하는 범국가적 긴급대비 및 대응체제를 마련하는 것임
 - 이를 위해서는 1) 사후복구계획과 관련된 목표를 설정, 2) 계획의 범위 명시, 3) 관련기관으로부터의 지원, 4) 보고체계, 5) 경보체계, 6) 보안 사고 평가, 7) 대응결정, 8) 연락체계, 9) 긴급계획의 개정 등이 포함되어야 함

제5장 물류보안산업 전망 및 육성방안

1. 물류보안산업 동향 및 규모

1) 물류보안산업의 최근 동향

- 2001년 9·11 테러 이후 물류보안산업이 급성장하고 있음
 - 각국이 물류보안조치를 강화하고, 이에 소요되는 인적·물적 시스템을 개발하면서 하나의 거대한 ‘물류보안시장’이 형성되고 산업으로 발전하고 있음
 - 미국의 항만보안법 제정과 시행 등에 따라 물류보안시장은 더욱 확대될 것으로 전망되고 있음
 - 컨테이너 보안 장비(CSD) 및 컨테이너 검사장비, 전자 태그(RFID) 및 스마트 컨테이너 등 물류보안 시장의 규모는 2010년에 연간 90억 달러에 달할 것으로 예상되고 있음
- 글로벌 기업의 물류보안시장 참여가 가속화되고 있음
 - 국제적인 군수기업체인 록히드 마틴 그룹은 스마트 컨테이너 관련 기술의 개발과 보급을 주도해 온 사비 테크놀로지(Savi Technology)사를 인수하고, GE 등은 국제컨테이너보안협회(ICSO)를 창설하는 등 물류보안 시장에 적극적으로 참가하고 있음
 - 록히드 마틴 그룹과 GE 등 글로벌 기업이 물류보안 시장을 장악하기 위해 치열하게 경쟁하고 있는 이유도 물류보안산업의 성장 가능성이 매우 높기 때문임
- 글로벌 물류 솔루션 시장의 성장 가능성이 특히 높음
 - 물류보안산업 분야 중 현재 시행되고 있거나 향후 도입이 예정되어 있는 물류보안제도 관련 시설 및 장비, 그리고 정보통신산업(IT)에 기반을 둔 보안 솔루션 분야의 성장 가능성이 무궁무진하다는 평가를 받고 있음
 - 특히 컨테이너 화물에 들어있는 위험화물을 가려내는 장비와 제조업체 또는 항만 터미널 등 물류 핵심시설에 대한 비인가자 출입을 통제하는 시스템 등이 주요 대상임

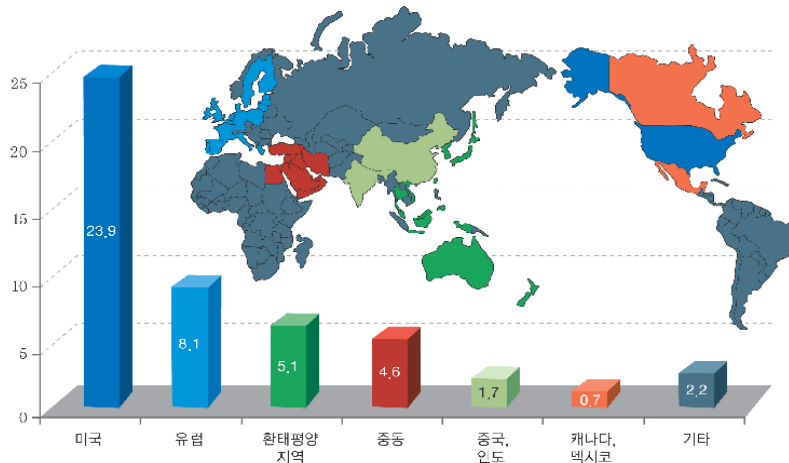
2) 글로벌 물류보안산업 규모

- 물류보안산업의 시장규모는 2005년 기준으로 약 464억 달러 정도로 추산되고 있음
 - 지역별로 살펴보면, 미국 시장이 239억 달러로 세계시장의 약 52%를 차지하고 있으며, 유럽이 81억 달러, 호주를 포함한 일본, 한국 등 환태평양 지역이 51억 달러, 중동 지역이 46억 달러, 중국과 인도가 17억 달러, 캐나다 및 멕시코 지역이 7억 달러이며, 나머지 지역이 22억 달러 정도로 추산되고 있음

<요약 그림-7>

세계 보안산업 시장규모(2005년)

단위 : 10억 달러



- 컨테이너 검색기 시장의 규모는 2006년에 미국기준으로 3억 8천만 달러에 달한 것으로 추정됨
 - Frost & Sullivan은 미국 컨테이너 검색기 시장의 규모가 2006년 3억 8천만 달러에서 2013년에는 12억 7천만 달러로 증가세를 나타낼 것으로 예상했음
- 컨테이너 보안장치(CSD) 시장은 미국 항만보안법 시행으로 50억원 상당의 엑스레이 검색대 소요량이 급증할 것으로 전망되고 있어 향후 급속한 팽창이 예측됨

- 예를 들어 우리나라의 대미 수출 화물량을 기준으로 할 때, 부산항에서만 최소 1천억 원 이상의 비용이 발생할 것으로 분석됨
- 스마트 컨테이너 시장은 2006년 7천만 달러에서 2012년에는 42억 달러에 이를 것으로 예측됨
 - 또한 2006년과 2012년 사이에 해운 컨테이너 보안 분야에 120억 달러가 지출되고, 지상용 커맨드, 컨트롤 통신 인프라에 약 7억 달러가 추가적으로 지출될 것으로 전망됨

3) 물류보안산업의 적용 부문

- 물류보안에 영향을 끼치는 핵심 요소에 근거하여 물류보안 적용산업은 크게 6가지로 구분될 수 있음
 - 즉 시설관리, 화물관리, 인적관리, 정보 및 커뮤니케이션 관리, 비즈니스 네트워크 및 기업보안 관리시스템, 위기관리 및 재난복구 관리 부문 등이 해당됨

4) 주요 물류보안 기술 발전 및 경쟁력

- 전자봉인장치를 개발하는 업체는 아직 국내에 없음
 - 컨테이너 봉인장치 기술은 단순 개폐여부의 단순 정보만 활용하는 바코드 봉인 장비들이 점차적으로 RFID를 기반으로 한 전자 봉인장비로 전환되고 있음
 - 전세계적으로 전자 봉인장치(electronic seals)를 생산하여 판매하고 있는 기업은 Arbic Berhad, Harcor Security Solutions, Hi-G-Tek Ltd, Leghorn, Unisto Limited 등이 있으나 국내 기업은 없음
- 핵물질 감지기술은 아직 신로도가 낮고 일부 수작업도 요구되는 등 기술개발 여지가 많음
 - 방사선을 이용한 핵물질 감지기술은 폴리비닐 톨루엔(Polyvinyl toluene)을 사용한 광자(photons) 탐지 방법이 20년 이상 사용된 기술로 신뢰도가 낮음
 - 현재 컨테이너 내부를 영상으로 검색하는 장비는 X-선 혹은 감마(Gamma)-선을 이용하는 기술이 활용되고 있으나, 낮은 투과성으로 인

- 해 100% 검색은 불가능하며 이를 보완하기 위해 수작업을 병행하고 있어 검사 속도가 낮은 단점이 있음
- 연구핵심은 16인치 두께의 철을 통과하는 투과성 기술을 확보하여 검사 시간을 줄이는 데 있음

2. 물류보안산업 지원·육성 방안

1) 정책 목표와 수단

- 물류보안산업의 육성을 위해서는 물류보안산업 지원제도 완비, 물류보안 산업 인프라 장비, 물류보안업체 역량강화 등이 1차적으로 요구됨
- 그리고 물류보안산업의 지원제도는 국가 물류보안계획 수립, 물류보안 인력양성지원, 물류보안 국제협력체제 구축 등을 들 수 있음
- 물류보안업체의 역량 강화는 물류보안 기술개발, 장비, 인력, 연구역량, 컨설팅, 네트워크 등이 다른 국가보다 우위에 있도록 해야 함

2) 물류보안산업 육성을 위한 산업구조정책

- 산업구조 정책수단은 1) 하부구조의 구축, 2) 성장잠재력 개발, 3) 기술혁신 등임
- 우선 하부구조의 구축을 위해서는 개별 민간기업의 업무범위를 넘어서 국가 또는 관련 단체에서 기획, 설계, 시공, 운영하는 등 모든 업무를 관할하여야 함
- 현재 물류보안은 연 평균 7~8%의 성장률을 기록하고 있는 유망산업으로서 정부의 다양한 지원정책이 필요한데, 특히 산·관·학의 연구사업을 통한 기술 혁신이 요청되고 있음

3) 물류보안산업 부문별 지원 방안

- 우선 컨테이너 전자 봉인장치 부분에서는 Savi나 GE사의 제품이 시장에서 주도권을 쥐고 있으므로, 이보다 성능이 우수하거나 가격 경쟁력에서 우위를 확보할 수 있는 기술 개발이 필요함
- 이를 위해서는 산학연 협동 체제를 구축하여 원가를 낮추는 기술개발과

이를 위한 저금리 자금 지원이나 파이낸싱 등을 정부차원에서 지원할 필요가 있음

- 컨테이너 화물 검색기 시장은 컨테이너 화물 100% 검색 의무화 법률이 미국 내에서 통과함으로써 향후 그 시장이 급속히 확대될 것으로 판단됨
 - 정부는 보안 관련 장비 및 시스템의 도입에 따른 재정적 부담을 최소화하기 위해 보안 할증료 제도를 정비하고 지속적인 지원책을 마련해야 함
 - 또한 우리나라에서 개발되고 있는 제품이 상용화되어 해외에 수출할 수 있도록 산업계 및 학계와의 연계를 강화하고 제품개발 자금 지원 및 민간자본 투자 중재 등을 고려할 필요가 있음
 - 특히 미국 SAIC사 제품의 경우 X선 검색기에서 발생하는 방사선 피폭 때문에 미국 동부 항만의 차량 기사들이 검사기 통과를 기피하는 사례가 발생되고 있어 우리나라 업체에서는 이를 보완할 수 있는 기술개발이 요구됨
 - 그리고 국내기업이 개발한 컨테이너 화물 검색기가 전세계적으로 판매되기 위해서는 미국의 표준과 일치해야 하고 또한 인증도 필요하기에 이에 대한 정부 지원이 필요함
- 컨테이너 화물 추적 장치의 경우 그 시장규모가 전 세계적으로 약 40억 달러에 달하고 있음
 - 정부는 스마트 컨테이너와 관련된 기술을 개발하고 있는 산업계와 연계하여 우리나라 성장 동력산업으로 채택하는 한편,
 - 세제 혜택이나 연구개발의 적합성을 판단하여 자금지원, 파이낸싱 등의 재정적 지원이 가능하도록 하는 제도적 장치마련이 필요함
- 물류보안 기술개발 연구사업을 위해 정부는 우선 물류보안산업 육성을 위한 기본계획을 마련하고 연구기술 개발을 위한 세부전략을 마련해야 함
 - 특히 물류보안기술개발 업체에 대한 지원책으로 현재 유전 개발 등 해외 자원개발사업 등에 활용하고 있는 ‘성공불 용자’ 도입이 필요함
 - 성공불 용자란 대규모 투자가 필요하나 투자금 회수 기간이 길고 리스크는 높은 사업에 대해 자금을 빌려준 뒤, 성공하면 원리금에다 특별 부담금까지 받지만 실패할 경우에는 원리금 상환부담을 대폭 경감해 주는 제도임

- 물류보안산업이 확산되면서 물류보안교육 및 컨설팅 부문의 성장이 예고되고 있음
 - 현재 물류보안제도는 미국에 의해 주도되고 국제기구에서 수용하면서 확산되고 있으나, 우리나라에서는 현재 물류분야의 컨설팅은 주로 IT 분야와 물류시스템 개선분야에 집중되고 있음
 - 물류보안교육 및 컨설팅 분야에서는 1) 물류보안교육 프로그램 개발 및 지원, 2) 물류보안교육에 대한 교육비 지원, 3) 물류보안 컨설팅 업체에 대한 지원 등과 같은 지원방안이 마련되어야 함

제6장 결론 및 정책 제언

1. 연구 결론

- 2006년과 2007년 2년 동안 연구를 수행한 결과와 앞으로 우리나라가 물류보안제도를 확립하는 데 필요한 정책적 시사점은 다음과 같은 6가지로 요약할 수 있음
 - 첫째, 2001년 9·11 테러 이후 물류보안이 글로벌 트렌드로 정착되면서 국제 교역에 상당한 영향을 미치고 있음
 - 둘째, 최근 미국을 비롯해 국제기구들이 물류보안을 더욱 강화하고 있는데, 이 같은 기조는 앞으로도 한동안 지속될 것으로 보임
 - 셋째, 주요 국가들은 최근 들어 WCO의 SAFE Framework 등 물류보안 인증제도를 속속 도입하고 있어 이에 대한 대책도 시급함
 - 넷째, 물류보안이 국제적으로 확산되면서 미국을 포함한 일부 국가와 글로벌 기업들이 이에 관련된 정보를 과점화하는 현상도 필요한 것으로 판단됨
 - 다섯째, 또한 국제적으로 물류보안제도가 확산됨에 따라 전자 태그 등 물류보안 시장도 급성장하고 있어 이를 활용한 전략도 필요한 것으로 판단됨
 - 여섯째, 국제적인 추세에 견주어 봤을 때 우리나라의 물류보안제도 이행

은 중간수준인 것으로 평가돼 앞으로 이 부분에 대한 제도 개선과 투자가 시급한 실정임

2. 정책 제언

1) 국가 물류보안계획 수립·시행

- 국가 물류보안 계획 주요 내용에 대한 제언은 다음과 같음
 - 1) 우리나라 물류보안에 관한 기본 방침, 2) 중장기 정책방향, 3) 각 부처별 국가 물류보안체제 구축에 관한 사항, 4) 물류보안 인프라 구축에 관한 사항, 5) 물류보안 전문인력 양성, 6) 물류보안 연구개발 추진, 7) 물류보안산업 육성 및 지원에 관한 사항, 8) 테러 사태 발생에 따른 신속한 대응방안, 9) 물류보안에 관한 국제협력 등임

2) 물류보안 관련 법률의 개선

- 우선 국제선박 및 항만시설 보안에 관한 법률을 개정하여 범 부처간 물류보안 업무를 통합 및 조정하는 규정을 삽입하는 방법과
- 가칭 ‘물류보안 촉진 및 지원에 관한 법률’을 신규제정하는 방법을 고려할 수 있음
 - 이 경우 1) 법률의 제정목적, 2) 물류보안에 관한 정부 및 민간부문의 의무와 책임, 3) 이 법률에서 사용되는 용어에 대한 정의, 4) 물류보안에 관한 각 정부 부처의 권한과 관장업무, 5) 각 부처 차관 급으로 구성되는 물류보안위원회의 설치·운영, 6) 국가 물류보안 계획의 수립·시행, 7) 물류보안 인증제도의 도입, 8) 물류보안 조사 및 연구 개발, 9) 물류보안 전문 인력의 육성, 10) 물류보안 참여업체에 대한 지원, 11) 물류보안 장비 및 기술 개발 투자와 지원, 예산의 확보, 12) 물류보안 정보시스템 구축, 13) 국제 물류보안 협력 등에 관한 사항이 포함되어야 할 것임

3) 물류보안 인증제도의 도입

- 물류보안 인증제도를 도입하는 것으로 목표로 다음과 같은 준비작업이 필요할 것임

- 1) 법적인 근거 마련, 2) 인증에 참여하는 기업이나 단체의 범위 설정, 3) 참여 대상 기업이 준수해야 할 물류인증기준 마련, 4) 물류보안 심사 기관의 선정, 5) 물류보안 인증업무의 대상 주무부처의 결정 등임

4) 완벽한 물류보안 시스템 구축

- 이를 위해서는 인적 및 물적 보안시스템 마련을 위한 ‘물류보안 패키지 시스템’ 구축이 필요함
 - 즉 산자부, 정보통신부 등 유관 정부간 협의를 거쳐 물류보안제도가 요구하는 사양의 시스템 구축이 필요함

5) 물류보안산업의 육성 및 지원

- 완벽한 물류보안 시스템을 구축하기 위해서는 이에 걸 맞는 기술과 장비 및 소프트웨어 등 일정한 물류보안 솔루션을 개발하고 보급하는 것이 중요함
 - 이를 위해서는 1) 스마트 컨테이너의 개발, 2) 컨테이너 화물 검색기 시스템의 개발 등에 대한 기술 개발 지원이 필요함
 - 국제 표준기구 등과 함께 컨테이너 화물 검색기 및 스마트 컨테이너에 대한 국제 표준을 우리나라 주도로 수립해야 함

6) 국가경쟁력에 물류보안을 활용

- 우리나라 항만에 완벽한 물류보안 시스템을 갖추는 경우 우리나라 항만의 경쟁력이 높아질 뿐만 아니라 중국 환적 물동량을 유치하는 데도 기여할 것임
 - 우리나라 항만에 물류보안 시스템을 신속하게 구축하여 항만 마케팅 등에 적극적으로 활용할 필요가 있음

7) 물류보안 연구센터 설립·운영

- 물류보안의 강화와 확대에 대비하기 위해서는 일반적인 행정기구와 더불어 전문연구센터가 필요함
 - 물류보안은 국제물류, 테러와 보안기술, 정보화와 IT 등 최첨단기술, 국제 표준과 국제기구의 동향, 미국 및 EU의 보안동향 등 다방면의 전문지식과 기술을 요구하고 있음
 - 특히 우리나라에서 물류보안산업을 새로운 성장산업으로 육성하기 위해

서는 이와 같은 전문지식을 갖고 정책대안을 개발할 수 있는 전문연구조직이 필요함

- 따라서 정부의 물류보안을 전문적으로 연구하는 조직을 정부의 재정지원으로 운영할 수 있는 방안을 마련해야 함

8) 민간 부문의 부담완화도 필요

- 물류보안제도 도입 및 관련 시스템 구축 및 운영과정에서 상당한 비용이 소요되는데, 이 같은 부담의 상당부분 민간 기업의 지출로 이루어지고 있는 것이 현실임
 - 외국의 경우 대부분 선박이 입출항할 때 항만시설 보안료를 부과·징수하고 있는 것이 가장 큰 부담이며, 국제해사기구의 ISPS 코드를 이행하는 과정에서도 선박과 터미널 등에서는 연간 10만 달러 이상을 지출하고 있는 것으로 나타났음
- 앞으로 미국 등이 컨테이너 화물에 대한 100% 검색을 의무화하고, 이른바 ‘10+2’ 제도를 통해 화물에 대한 통제를 강화하게 되면, 제조업체 등 민간 기업이 부담해야 하는 지출은 더욱 늘어날 것이 확실함
 - 따라서 민간 기업의 부담을 줄이고, 국제경쟁력을 확보하기 위해서는 물류보안 인프라 구축 및 운영 등에 소요되는 비용에 대해서는 원칙적으로 국가가 부담하는 것으로 하고,
 - 물류보안 인증제도 등을 시행할 때는 인센티브를 제공하는 유인책과 부담 경감방안을 동시에 고려할 필요가 있음

3. 정책 추진 일정표

- 이 같은 연구결과를 토대로 앞으로 정부 및 민간 부문에서 활용 가능한 정책 대안과 이를 추진하는 데 필요한 업무 일정표(로드맵)를 제시하면 다음과 같음

<요약 표-4>

정책 제언 사항 추진 로드맵

정책 제언 사항	추진 시기			추진방법
	2008년 까지	2010년 까지	2012년 까지	
1. 국가물류보안계획 수립·시행	○			관련부처 법정계획으로 추진
2. 물류보안 관련 법률 제·개정		○		해양수산부, 건설교통부 등이 신법 제정
3. 물류보안인증제도 도입·시행	○			관세청·해양수산부, 건교부 등이 기준 제정 후 사업 시행
4. 완벽한 물류보안시스템 구축		○		항만부터 시스템 구축 후 전 물류구간으로 확대
5. 물류보안산업의 육성·지원	○	○	○	가능한 사업부터 단계적으로 추진
6. 국가경쟁력에 물류보안 활용		○		제시한 국가 물류보안계획에 반영하여 추진
7. 물류보안연구센터 설립·운영	○			물류보안전문연구기관 조직으로 설립

자료 : 한국해양수산개발원

제1장 서론

1. 연구의 배경과 목적

1) 연구 배경과 필요성

물류보안¹⁾이 글로벌 메가 트렌드(global mega trend)로 정착되고 있다. 2001년 미국에서 발생한 9·11 항공기 테러 이후 주요국들이 물류 전 구간의 보안조치를 크게 강화하고 있기 때문이다. 특히 미국을 비롯한 국제사회는 최근 들어 기존의 물류보안 조치를 강화하는 한편, 국제적인 협력과 연대를 바탕으로 통일된 물류보안 인증제도를 도입하고 있다.

미국은 18개 부처에 분산되어 있던 보안 관련 기능을 통합한 국토 안보부(DHS)를 2003년에 창설한 이후 컨테이너 보안 협정(CSI), 대테러 민·관 협력사업(C-T PAT) 및 해운보안법의 제정 등을 통해 물류부문의 보안을 강화하기 위한 기초를 다졌다. 특히 2006년 9월 13일에는 항만보안법('SAFE Port Act')을 제정해 물류보안을 더욱 강화한다는 의지를 대내외에 다시 한번 천명하였다.

이 같은 상황에서 미국은 2007년 8월에 물류보안을 획기적으로 강화하는 새로운 제도를 도입하였다. 미국의 조지 W 부시 대통령은 8월 3일, 2007년 1월과 7월에 미 하원과 상원이 각각 통과시킨 이른바 수출 컨테이너 화물의 100% 사전 검색을 의무화하는 법률을 최종적으로 확정·공포하였다.²⁾ 이에 따라 세계 각국에 직접적으로 영향을 미치는 미국의 물류보안제도는 당분간 더욱 계속될 것이 거의 확실하다는 관측이 전문가들 사이에서 나오고 있다.

미국을 중심으로 시행되기 시작한 이 같은 테러 예방 및 물류보안제도는 양자 및 다자기구로 확산되면서 글로벌 제도로 정착되고 있는 것도 새로운 현상이다. 국제해사기구(IMO)와 국제노동기구(ILO), 그리고 경제개발협력기구(OECD) 등 국제기구는 미국과 유사한 제도를 도입하여 전 세계적으로 동일한 기준에 따라 물류보안을 더욱 확대하고 있다. 이에 따라 물류보안제도가 초기의 항만이나 선박을

1) 이 용어는 Supply Chain Security를 우리말로 옮긴 것으로 일부에서는 물류 안전 또는 화물 안전, 물류 공급망 안전이라고 표현하기도 함.

2) 이 법률의 정식 명칭은 '9·11 테러 대책 위원회의 권고를 이행하는 2007년 법률(The Implementation Recommendations of the 9/11 Commission Act of 2007)임.

중심으로 이루어지던 단계에서 벗어나 물류 전 구간으로 확대되고 있으며, 개별 국가 위주에서 글로벌 기준으로 정착되고 있다.

IMO의 경우 2004년 7월에 선박 및 항만시설의 보안을 강화하는 이른바 ISPS Code³⁾를 도입한 데 이어 2005년에는 선박과 해양시설 등에 대한 테러 예방과 진압을 목적으로 하는 새로운 협약을 제정하였다.⁴⁾ 이 협약은 그 동안 국제사회에서 크게 문제가 되었던 이른바 대량살상무기(WMD)를 적재한 선박을 해상에서 승선·검색하는 것을 핵심으로 하는 PSI 관련 규정을 두고 있다. 이에 따라 협약의 이 같은 조항은 앞으로 발효 및 시행과정에서 뜨거운 감자로 등장할 가능성도 있는 것으로 판단된다.

OECD와 세계관세기구(WCO), 아시아·태평양 경제협력체(APEC) 등 국제기구도 해운·내륙·항공 등 3개 운송부문의 완벽한 보안확보와 수출입화물의 안전한 통관을 보장하는 새로운 제도를 도입하고, 국제적인 시행방안을 마련하고 있다. 특히 WCO는 2005년 10월에 채택한 「국제교역의 안전과 간소화를 위한 국제기준」⁵⁾을 통해 세계적으로 동일한 물류보안 인증제도를 도입하기 위해 적극 나서고 있다.

유럽연합(EU)도 2006년 12월에 제조업체와 해운회사 등 관련 업계의 강력한 반대에도 불구하고, WCO의 물류보안 인증제도를 기반으로 하는 ‘물류보안 인증 사업자 제도(Authorized Economic Operator : AEO)’를 도입하여 2008년부터 본격적으로 시행한다는 방침이다. 특히 유럽연합의 경우 2007년 1월에 회원국 수가 모두 27개 국가로 확대되었다. 이에 따라 유럽연합이 물류보안 인증제도를 시행하는 것은 앞으로 유럽연합 역내뿐만 아니라 우리나라 등 다른 나라의 컨테이너 교역에 미치는 영향이 매우 클 것으로 분석되고 있다.

싱가포르 또한 2007년 5월 25일부터 ‘물류보안 파트너 십 제도(STP6)’를 공식적으로 도입하여 시행하고 있다. 이 제도는 물류산업에 종사하는 모든 기업들이 물류보안을 확보하는데 필요한 기준과 인증절차를 규정하고 있다. 싱가포르는 2006년 7월 자국에서 개최한 APEC 물류보안 총회에서 기존의 물류보안제도를 포괄적으로 아우르는 통합물류보안제도를 도입할 계획이라고 밝힌 바 있다.⁷⁾ 아시아 국

3) 이 용어의 정식 명칭은 International Ship and Port Facility Code임.

4) 해상불법행위 억제에 관한 2006년 IMO 협약을 말함.

5) 이 제도의 정식 명칭은 Framework of Standard to Secure and Facilitate Global Trade : SAFE Framework임.

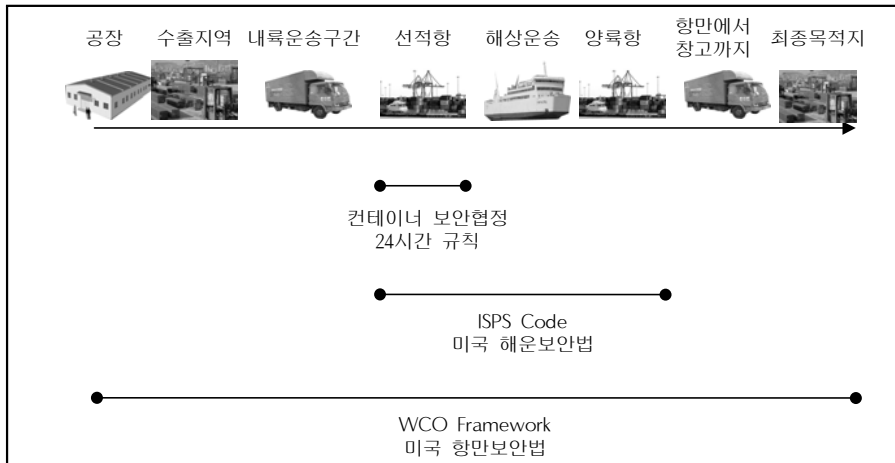
6) 이 제도의 공식 영문 명칭은 ‘Secure Trade Partnership Programme’으로 싱가포르는 이 제도를 정식 도입하기에 앞서 자국내 8개 기업을 대상으로 시범 사업(Pilot Programme)을 진행하였음.

7) 한국해양수산개발원, 지구촌해양수산(해운항만), 제15집, 2006. 12.

가로서는 처음으로 싱가포르가 이 같은 제도를 도입함에 따라 홍콩 등 다른 나라들도 같은 대열에 합류할 가능성이 매우 커졌다.⁸⁾⁹⁾

<그림 1-1>

물류보안제도 적용 범위 및 확대 동향



자료 : 한국해양수산개발원

문제는 국제적인 상황이 이런데도 불구하고, 우리나라의 경우 일부 정부 부처를 제외하고는 여전히 물류보안에 대한 이해와 인식이 크게 부족하다는 점이다. 우리나라 선사나 기업들은 물론 정부 부처 또한 물류보안을 부담 요인으로 인식하고 있으며, 수동적인 자세에서 제도를 부분적으로 이행하고 있기 때문이다. 특히 우리나라 각 부처의 경우 물류보안과 관련된 소관 업무만을 처리할 뿐 물류 전 구간을 통합적인 차원에서 처리하는 물류보안 정책이 거의 없는 실정이다. 그나마 다행인 것은 해양수산부가 2007년 2월 경제정책 조정회의에서 ‘국제물류보안 강화추세를 활용하는 보안 서비스 개발’이라는 정책¹⁰⁾을 마련하였다는 점이다. 해양수산부는 앞으로 이 정책을 토대로 보다 구체적인 물류보안 시스템 구축과 수익(비즈니스) 모델 등을 개발한다는 방침이다.

8) APEC도 2007년 들어 물류보안 연구그룹 회의를 잇달아 개최하면서 테러 이후 신속한 교역 재개 방안을 마련하는 한편, 각국에서 활용할 수 있는 물류보안 지침(가이드라인)을 작성하였음.

9) 뒤에서 살펴보는 바와 같이 뉴질랜드는 2007년 7월 3일 미국과 물류보안 인증제도를 서로 인정하는 내용의 협정을 체결했는데, 이 같은 협정은 WCO의 SAFE Framework에 기초한 최초의 양국간 물류보안 인증 협력이라는 점에서 관심을 끌고 있음.

10) 해양수산부의 이 같은 물류보안대책은 2007년 2월 2일에 의결된 ‘국가 해상물류 서비스 산업 경쟁력 강화 방안’에 포함되어 있음.

이 같은 국제적인 흐름과 추세를 고려할 때 우리나라 정부 및 민간 기업에 대해 정확한 물류보안 정보를 분석하여 제공하는 것이 무엇보다 시급한 과제로 등장하게 되었다. 현재 국제적으로 강화되고 있는 물류보안이 테러 예상이라는 본래 목적과 함께 국가 경쟁력을 확보하는 중요한 요소로 대두되었을 뿐만 아니라 화물의 신속한 통관이라는 국제 교역에 미치는 영향이 더욱 커지고 있기 때문이다.

또한 이 같은 물류보안 정보 제공뿐만 아니라 정부와 기업의 대응전략을 수립하기 위해서는 각 부문에서 무엇을 어떻게 해야 하는지 방향을 제시할 필요성도 커졌다. 물류보안이 2001년 9·11 테러 이후 국제적으로 다양한 방법으로 도입되고 있으나 아직 정부 및 민간 부문에서는 그 실체를 정확하게 파악하지 못하고 있고, 강 건너 불처럼 등한시하고 있기 때문이다. 즉, 1) 물류보안에 대한 정확한 정보의 제공과 2) 그에 따른 정부와 민간 기업의 대책 수립 지원이라는 화급한 과제를 해결하기 위해 이 연구를 수행하였다.

2) 연구 목적

이와 같은 현실 인식을 바탕으로 이 연구에서는 크게 다음과 같은 두 가지 목적을 설정하고, 2006년부터 2개년도 사업계획으로 연구를 진행하였다.

첫째, 2006년 제1차 연구에서는 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 정착되고 있는지 집중적으로 분석하였다.

둘째, 2007년 제2차 연구에서는 1차 연구에서 파악된 우리나라 물류보안제도의 문제점을 중심으로 국제적인 동향과 향후 전망에 맞춰 앞으로 기존 제도를 어떻게 개선해야 하는지 검토한 다음 국가 물류보안체제 구축 방안을 제시하는데 연구의 초점을 맞추었다.

특히 2차년도 연구에서는 국가 물류보안체제를 구축하는데 근간이라고 판단되는 물류보안제도 개편 방안과 물류보안 기술 및 장비 개발 등 관련 산업을 육성하는 방안에 초점을 맞추고 연구를 진행하였다.

2. 선행연구 내용의 분석

1) 1차년도 연구 내용

이 연구는 2년 계획으로 진행하고 있다. 2006년에 수행된 제1차 연구는 총론에 해당된다. 주로 테러리즘에 대한 원인 분석과 테러가 발생하는 경우 물류부문에 미치는 영향 등을 분석하였다. 또한 9·11 테러 이후 국제사회에서 도입되고 있는 여러 가지 보안제도 등에 대해서도 심층적으로 검토하였다. 우리나라의 기존 보안제도와 물류보안제도와의 차이점 등도 살펴보았다.

이 같은 검토를 토대로 물류보안제도가 앞으로 글로벌 메가 트렌드로 정착될 것이라는 판단에 따라 대비책을 마련하는 것이 시급하다는 결론을 이끌어냈다. 연구 진행과정에서 자문에 응한 많은 전문가들이 컨테이너 화물의 안전성 확보가 앞으로 상당기간 국제적인 중요 현안으로 대두될 것이라는 데 의견을 같이 하였다. 이에 따라 세계적인 물류보안 강화 동향을 수동적으로 받아들이기 보다는 적극적으로 활용하는 전략이 절실하다는 입장을 피력하였다. 또한 우리나라의 항만 경쟁력 확보와 물류 서비스 고도화를 위해서는 국가 물류보안 전략이 필요하다고 제안하였다.

제1차년도 연구보고서에서는 향후 우리나라 물류보안 정책 방향을 다음과 같이 제시하였다. 첫째, 물류보안이 확산되는 초기단계에서 완벽한 보안시스템을 구축하고, 필요한 제도를 마련하는 것이 앞으로의 국제적인 물류 경쟁에서 유리하다. 둘째, 물류보안산업을 육성하고, 관련 기업이 세계시장에 진출할 수 있도록 성장 기반을 구축하는 것도 시급하다. 셋째, 우리나라 물류보안제도를 세계화하는데 해운회사 등 관련업계에서 입을 수 있는 부담을 최소화하고, 제도 확산을 위한 일정한 인센티브를 도입할 필요가 있다는 점도 지적하였다.

그리고 이 같은 기본 방향에 따라 앞으로 우리나라는 다음과 같은 세 가지 틀에서 물류보안정책을 추진하는 것이 바람직하다고 제시하였다. 첫째, 우리나라 물류보안체제를 세계화하는 것이 시급한데, 그 대안으로, 1) 국가 물류보안 협의체 구성·운영, 2) 고성능·최첨단 항만보안 시스템 확보, 3) 완벽한 통합 물류보안 시스템을 구축해야 함. 둘째, 물류보안의 고도화·고품격 서비스화로 우리나라 항만 및 물류 경쟁력을 확보해야 하는데, 그 대안으로 1) 물류보안 인증제도 도입, 2) 주요국과 화물 신속통관 협정 체결, 3) 환적 화물에 대한 보안인증제 도입 등을

제안하였음. 마지막으로, 물류보안을 새로운 성장 동력으로 활용하는 전략을 개발해야 하는데, 그 대안으로 1) 물류보안 장비·기술을 표준화하고, 2) 물류보안 정보 수집 및 활용 능력을 제고하는 것이 시급하다고 강조하였음. 제2차년도 연구는 이 같은 사항을 보다 구체화할 수 있도록 국가물류보안계획(안)을 제시하고, 물류보안산업을 육성·지원하는데 역점을 두었다.

2) 주요 선행연구 검토

2001년 9·11 테러 이후 국제적으로 물류부문의 보안에 관한 관심과 우려가 증폭되고 있는 것이 오늘의 현실이다. 그러나 아쉽게도 아직 우리나라의 경우 통합적인 시각에서 물류보안에 관한 연구가 거의 이루어지지 않고 있는 실정이다.

다만, 예외적으로 국제해사기구(IMO)가 제정한 ISPS Code를 시행하기 위해 해양수산부가 관련 연구(「ISPS Code 시행방안 대비 국제협력 방안 연구」, 2004년)를 진행하였다. 이 연구는 2004년 7월부터 국제적으로 시행되고 있는 국제협약의 국내 이행절차를 마련하는 것에 연구의 초점을 맞추고 있다. 해양수산부는 이 연구를 토대로 ISPS Code를 우리나라에서 이행하는데 필요한 고시를 제정하여 시행하고 있다. 또한 이 고시를 수정·보완한 것이 2007년 7월 2일 국회에서 통과된 ‘국제 항해선박 및 항만시설 보안에 관한 법률’이다.¹¹⁾

이 밖에도 해양수산부는 「ISPS Code 시행에 따른 항만보안관리제도의 제도적 개선방안」(2005)에 관한 연구도 수행하였다. 이 연구는 부산항의 보안·경비 조직과 항만 보안료 징수체계를 개선하는 것으로 연구 내용을 한정하고 있다.

이에 비해 본 연구는 각 부문별로 단편적으로 이루어지고 있는 물류보안 활동을 통합적이고, 국가 전체적인 차원에서 분석한 다음 정책 대안을 제시하는데 연구의 초점을 맞추고 있다. 선박이나 항만 등 컨테이너 화물을 운송하는데 관련되어 있는 물리적 수단뿐만 아니라 각 구간의 연계성을 살피고, 제도적인 흠결을 보완하기 위한 것이다. 2007년 5월 25일에 발표된 싱가포르의 통합물류보안계획(STP)도 이 같은 관점에서 수립되었다.

한편, 국외에서는 물류보안과 관련된 개별 논문들이 상당수 발표된 것으로 조사되었다. 예컨대, 태국의 타마삭 대학교의 루스 바노명이 발표한 “해운 공급 망 보

11) 이 법률은 기본적으로 ISPS 코드 이행에 관한 우리나라 고시를 법률화한 것이나 i) 국가항만보안계획의 수립 및 시행, ii) 항만시설 운영자에 대한 항만 보안료 징수 권한을 포함한 것이 특징임.

안조치로 인한 항만 및 교역 부문의 영향¹²⁾” 등이 대표적이라 할 수 있다. 또한 컨테이너 검색 제도를 집중적으로 분석한 연구 자료도 나와 있다. 2005년 5월에 미국의 랜드 코퍼레이션이 펴낸 ‘글로벌 컨테이너 공급망의 보안성 평가¹³⁾’가 그것이다. 이 보고서는 랜드 코퍼레이션이 자체적으로 수행한 컨테이너 보안 검색제도 소개서이다. 주로 이 보고서는 9·11 테러 이후 미국이 도입한 주요 컨테이너 보안조치를 소개하고, 컨테이너 화물의 위험 요소 분석 및 검색 방법, 장비, 기술 등에 대해 언급하고 있다. 또한 이 보고서는 현재 개발된 기술을 바탕으로 향후 컨테이너 보안 향상 방안을 제시하고 있다는 점에서 이 분야의 선도 연구 자료로 평가되고 있다. 다만, 이 연구는 현재 국제적으로 확산되고 있는 물류보안조치를 전체적으로 포괄하지 않고, 컨테이너 한 분야만을 다뤘다는 점에서 본 보고서와 차이점이 있다. 또한 이 보고서는 미국의 물류보안제도와 기술만을 소개하는데 그친 것이 한계점으로 평가된다.

또한 최근에 물류보안이 강화됨에 따라 컨테이너 화물 검색기 등 관련 산업의 시장 전망 등을 분석한 보고서들도 다수 발간되고 있다. 이들 보고서들은 물류보안 시장에 참여하고 있거나 참여방안을 검토하고 있는 기업들을 대상으로 하고 있어 발간 가격이 600만원 이상의 고가로 책정되어 있는 것이 특징이다. 이와 관련된 서적으로는 「2004-2012 Maritime Smart Container Market/Technology Forecast Report(Homeland Security Research Corp. Sep 2004)와 「Container Security-A Market Analysis(Frost and Sullivan, 2007)」 등이 대표적이라고 할 수 있다. 전자는 주로 차세대·최첨단 컨테이너 화물 운반용기로 부상되고 있는 이른바 스마트 컨테이너의 개념과 이에 소요되는 기술과 장비, 그리고 현재 및 향후 시장규모 등을 추정한 보고서이다. 본 보고서가 향후 관련 업계의 수익 모델의 하나로 스마트 컨테이너 개발·보급 문제를 검토하였다는 점에서 접근방법에서 일부 유사성이 있다. 후자는 컨테이너 보안에 관한 시장 전망을 분석한 보고서이다. 컨테이너 검색장비 시장, 컨테이너 전자 봉인 시장, 그리고 컨테이너 모니터링 시장 등 3분야의 물류보안 시장의 현황과 트렌드, 시장 경쟁 상태 등을 집중 분석한 것이 특징이다. 특히 이 보고서는 각 장에서 컨테이너 검색 장비 시장(제2장), 컨테이너 봉인장치 시장(제3장), 컨테이너 추적(모니터링) 시장(제4장) 등 3개 부문을 집중적으로 조명하

12) Maritime Policy and Management, January-March, 2005.

13) Herry. H. Willis, David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, RAND Corporation, 5. 25, 2005.

고 있는 것이 특징인데, 각 장에서 현재의 시장 규모와 2006~2013년까지의 시장 성장 예측을 담고 있어 글로벌 물류보안 시장 규모를 이해하는데 도움이 된다. 또한 이 보고서는 각 부문별로 기술 개발 정도와 각각 기술을 보유 또는 상품화하고 있는 관련기업의 경쟁력까지 분석하고 있어 우리나라와의 물류보안 기술 격차를 비교·분석할 수 있는 참고자료로서도 가치가 있다. 본 보고서 제5장에 언급된 물류보안산업 육성 및 지원방안을 검토하면서 3가지 장비의 시장 현황과 기술 개발 수준 등을 주로 분석하였다.

3) 물류보안 국제회의 내용

물류보안이 강화·확산되면서 이와 관련된 국제회의나 세미나 심포지엄 등도 국내외에서 다양하게 열리고 있다. 우리나라의 경우 우리 연구원 등으로 포함해 한국선급, 한국무역협회가 공동으로 「2007 국제 물류보안 동향 및 대응전략 세미나(10월 23일, 트레이드 타워)」를 개최한 데 이어 12월 12일에는 민간 물류보안 정보 시스템 업체인 PNL 네트워크가 주관하는 「국제물류보안의 전망과 동향(Cargo Security Innovations)」이라는 세미나도 개최되었다. 후자의 세미나는 컨테이너 전자 봉인장치 및 화물 정보 시스템을 개발·판매하고 있는 사비 네트워크(Savi Networks)의 한국 파트너가 마케팅 차원에서 개최하였다는 점에서 새로운 현상으로 받아들여지고 있다. 외국 물류보안 기술업체가 우리나라에서 공식적으로 세미나 등을 개최하면서 시장에 진입하는 전략을 추진한 사례가 거의 없었기 때문이다.

한편, 해외에서도 다양한 주제를 놓고, 여러 가지 형태의 물류보안 세미나 등이 열렸다. 영국에서 발행되는 물류보안 전문지인 Cargo Security International 홈페이지에 게시된 자료에 따르면, 2007년 한 해 동안 국제적으로 개최된 물류보안 세미나나 워크숍 등은 30건이 넘는 것으로 파악되었다. 이 가운데, 지난 11월 7일부터 이틀 동안 아랍에미리트 두바이에서 열린 「Container Tracking & Security 2007」과 12월 5일~6일 사이에 미국 워싱턴에서 개최된 「6th Annual North America Cargo Security Forum」이 특히 관심을 끌었다.

두바이 물류보안 컨퍼런스는 물류보안의 법제도 부분과 기술 부분으로 나뉘어 이틀 동안 진행되었는데, 미국 CBP, 유럽위원회 및 디피월드, 허치슨 터미널, IBM, SAVI 등 물류보안 관련 정부기관과 민간기업 관계자가 다수 참석하였다. 세미나 내용에서는 제도분야의 AEO, C-T PAT, SFI 및 WCO Framework 등과 같은 주제가

발표되었다. 기술 분야는 컨테이너 보안장치(CSD) 및 전자 봉인장치(E-sealing) 분야의 현황 및 이슈 등이 집중적으로 발표되었다.

특히 이번 세미나에서는 홍콩, 영국의 사우스햄튼, 암스테르담항의 항만보안 사례와 미국 국토안보부(DHS) 및 일본의 소니 사 등 보안장치를 실제 사용하고 있는 기업들의 사례가 소개되어 눈길을 끌었다. 두바이 물류보안 세미나는 관련 정부기관 및 기업이 한 자리에 모여 물류보안이라는 주제를 다양하면서도 심도 있게 논의하였다는 평가와 더불어 컨테이너 보안장치 표준화 문제 및 미국 주도의 SFI와 WCO Framework의 갈등문제 해결 방안 등이 주로 거론되어 향후 이 분야에서 어느 정도 의견이 수렴될 수 있을지 관심이 모아지고 있다.

한편, 제6차 북미지역 화물보안 포럼에서는 지금까지 개최된 물류보안 국제회의와 약간 성격을 달리하는 방향에서 기획된 것이 특징이다. 즉 이 회의에서 다룬 주제는 물류보안에 관한 사항이 중심을 이루고 있었으나 화물 절도와 제조업체들이 국제간 화물 교역에서 어떻게 물류보안을 확보하고, 신속한 화물 흐름을 촉진하고 있는지 사례 발표가 다수 포함되었기 때문이다. 물류보안과 관련하여 두 가지 부문이 실제 업계에서는 가장 필요한 사항이기 때문에 이 같은 내용을 포함한 것으로 풀이되고 있다. 앞으로 우리나라가 물류보안을 확보할 때는 이 같은 경향도 참고할 필요가 있다.

3. 연구의 주요 내용과 수행방법

1) 연구의 주요 내용

이 연구는 크게 6개 장으로 이루어져 있다. 제1장 서론에 이어 제2장과 3장은 우리나라 물류보안제도를 개선하는데 필요한 총론적이며, 기본적인 사항을 주로 다루었다. 제4장과 제5장은 이른바 연구의 각론에 해당하는 부분으로 물류보안에 관한 제도와 기술 부분을 각각 언급하였다.

특히 제2·3장(최근의 물류보안 동향, 우리나라 물류보안시행 문제점)에서는 주로 1차년도 연구를 중심으로 주요국의 최근 물류보안 동향을 추가적으로 심층 분석하였다. 제1차년도 연구가 개별 국가와 국제기구의 물류보안제도를 분석하는데 중점을 둔 반면, 제2차년도 연구에서는 i) 선박 및 항만, ii) 컨테이너 화물 보안, iii) 물류보안 인증제도, 그리고 iv) 물류보안 기술 및 장비 등으로 카테고리를 구분

하여 최근의 변화를 세밀하게 파악하는데 역점을 두었다. 또한 이 곳에서는 제4장과 제5장에서 언급하는 우리나라 물류보안 확보 방안과 연결되는 향후 과제에 대해서도 언급하였다.

제4장에서는 우리나라 물류보안제도 개편 방안을 주로 검토하였다. 이에 따라 국가 물류보안체제를 구축하는데 기본적으로 필요한 국가물류보안계획의 수립에 관한 사항을 중점적으로 언급하였다. 국가 물류보안 계획에 반영되어야 할 기본 지침 및 중장기 정책 방향, 물류보안 인프라 구축 방안, 관련 기술 개발 및 산업 육성 방안 등이 제4장에서 중점적으로 검토되었다.

또한 제5장은 물류보안과 관련된 장비 및 기술, 표준 등에 관한 우리나라의 향후 정책 방안을 주로 다루는데 할애하였다. 특히 이 곳에서는 항만 및 물류 전구간을 포괄하는 물류보안 시스템 구축방안을 제시하는 한편, 컨테이너 화물 검색기 관련 사항과 2007년 5월 10일 국제표준화기구(ISO)에서 확정된 컨테이너 전자 봉인장치(E-seal) 표준을 우리나라에서 이행하는 방안 등 물류보안산업을 육성하고 지원하는 내용을 검토하였다. 또한 현재 국제적으로 급팽창하고 있는 물류보안 시장에 국내기업이 참여할 수 있는 부문에 대해서도 고찰하였다. 록히드 마틴이나 제너럴 일렉 트릭(GE) 등 글로벌 기업이 물류보안시장을 선점하기 위해 치열하게 경쟁하고 있는 이유도 이 곳에서 분석하였다.

제6장은 이 연구의 결론에 해당하는 부분이다. 지금까지 진행된 연구 내용을 정리하고, 앞으로 정부나 민간기업에서 추진해야 하는 정책들을 한데 모았다. 정책 건의가 바로 그것이다.

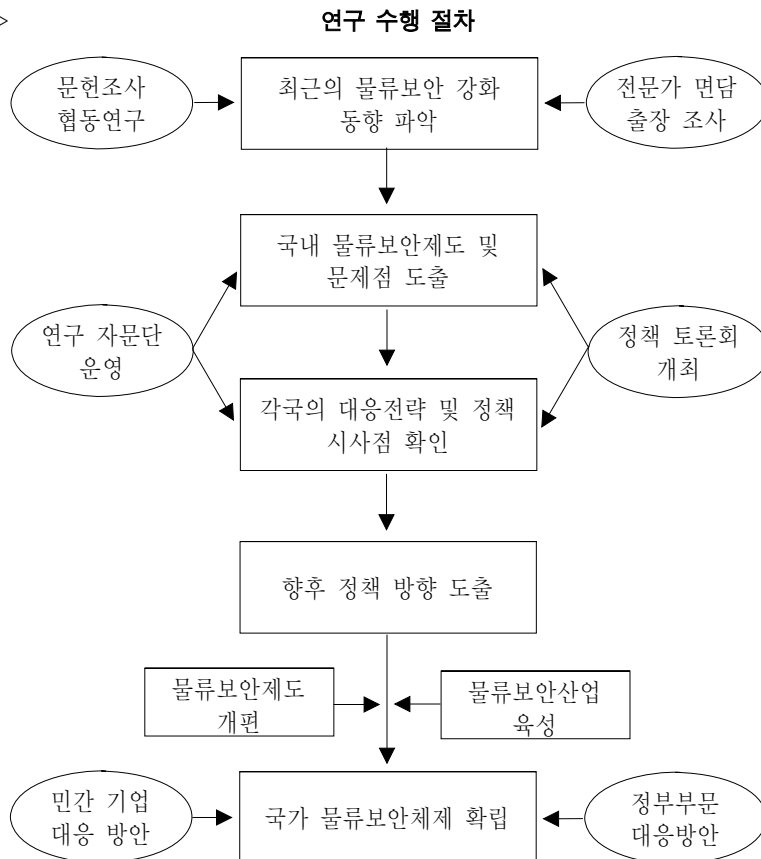
2) 연구 방법 및 절차

이 연구는 물류 전 구간에서 발생할 수 있는 테러와 같은 보안 사고를 사전에 예방함으로써 우리나라의 물류 시스템이 끊임없이(seamless) 운영될 수 있게 하는데 연구의 초점이 맞춰져 있다. 이 같은 연구 목적을 달성하기 위해서는 제도가 안고 있는 문제점과 직면하고 있는 실상을 정확하게 파악하고, 적절한 대책을 제시하는 것이 필수적이다. 물류보안과 관련되어 있는 정부 및 민간 부문과의 네트워크 구축과 정보 교류가 중요한 것도 이 때문이다.

이 연구에서는 우선 이 같은 점을 고려하여 관련 부문에 대해 외부 전문가와 협업 형태로 연구를 진행하였다. 특히 물류보안과 관련되어 있는 연구기관이나 정

부 부처와의 유기적인 협조체제를 구축한 상태에서 연구를 수행하였다. 국가정보원이 주관하고, 해양수산부·건설교통부 등 정부 부처와 한국선주협회, 한국무역협회 등 민간부문이 공동으로 참여하고 있는 ‘물류보안체제 구축 민·관 협의회’ 운영과 연계하여 연구를 진행한 것도 이 같은 이유 때문이다. 즉, 민간기업 등이 직면하고 있는 물류보안 애로사항을 신속하게 파악하고, 정부의 관련 정책 수립을 지원하는 것이 이 연구의 최종적인 지향점이기도 하다.

<그림 1-2>



둘째, 이 연구에서는 가능한 한 다양한 의견을 수렴하는데 주력하였다. 연구가 진행되는 기간 동안 착수, 중간 및 최종 보고회 등 모두 3회의 연구 보고회를 개최하는 등 관련 업계의 의견을 최대한 수렴하였다. 연구보고회에 참석하는 연구 심의위원을 각 분야별 전문가로 위촉하여 연구의 전문성을 제고하는 한편, 객관성을

확보하는데도 최대한 역점을 두었다.

셋째, 이와 함께 외국의 보안 전문가를 중심으로 인적 네트워크를 구축하고, 자료 수집과 자문에 활용하였다. 우리나라뿐만 아니라 외국의 제도 시행 동향에도 관심을 기울이고, 보고서의 질적 향상을 도모하는데 필요한 것으로 판단되었기 때문이다. 2007년 들어 APEC이 주도적으로 추진하고 있는 테러 이후 무역 재개 연구그룹 회의에 연구진을 주기적으로 파견한 것도 이와 관련이 있다.

넷째, 연구가 진행되는 과정에서 정부 및 관련 기업의 의견을 수렴하기 위해 관계 부처와 합동으로 물류보안제도 세미나를 개최하였다.¹⁴⁾ 이 보고서가 정부 정책 수립은 물론 기업이 앞으로 물류보안과 관련된 비즈니스 영역을 확대하는데 기여할 수 있는 보고서가 될 수 있도록 다양한 의견을 수렴하는 것이 바람직하기 때문이다.

다섯째, 그리고 우리 원이 기술적으로 접근하기에 한계가 있는 물류보안 기술 및 장비 개발 등에 관한 사항은 외부 전문가 협동 연구나 내부 세미나 등을 개최하여 연구 내용의 완성도를 높이도록 고려하였다. 제5장에서 중점 검토된 물류보안산업에 관한 사항은 인하대학교 협동연구진의 연구사항과 KPC 등의 세미나 결과를 반영한 것이다.

14) 이와 관련된 물류보안 대책 세미나는 산업자원부, 해양수산부, 건설교통부, 관세청, 국가정보원 등 정부 부처는 물론 한국무역협회, 한국선급 등 민간기관이 공동으로 참여한 가운데, 2007년 10월 23일 한국 무역협회 대회의실에서 개최되었음.

제2장 글로벌 물류보안제도 최근 동향

1. 선박과 항만 보안제도¹⁵⁾

현재 나와 있는 선박과 항만의 보안제도는 두 가지로 분류할 수 있다. 2002년에 만들어진 미국의 해운보안법(MSA 2002)과 국제해사기구(IMO)의 국제 선박 및 항만시설 보안에 관한 규칙(이하 'ISPS 코드')이다.¹⁶⁾¹⁷⁾ 전자가 미국의 개별적인 법률인데 비해, 후자는 2004년 7월 1일부터 국제적으로 시행되고 있는 국제규범이라는 점에서 차이가 있다. 그러나 IMO는 ISPS 코드를 제정할 당시 미국의 해운보안법을 모태로 활용하였다. 따라서 두 가지 규범은 일부 조항을 제외하고는 거의 유사한 것이 특징이다.

1) IMO ISPS 코드

ISPS 코드에 따르면, 선사 및 항만 당국, 그리고 체약국 정부는 선박과 항만의 보안을 확보하기 위해 여러 가지 의무사항을 부담해야 한다. 이 같은 사항 가운데 가장 눈에 띄는 점은 선박과 항만 시설에 대한 보안 계획의 수립과 이행에 관한 내용이다.¹⁸⁾

첫째, 국제항해에 종사하는 모든 선박¹⁹⁾은 체약국의 관련 관청에서 승인한 선박 보안계획을 비치하고, 운항해야 한다. 이 계획은 ISPS 코드에 규정된 3단계 보안 수준에 맞게 작성하도록 되어 있다. 선박 보안 1단계는 선박이 정상적으로 운영되

15) 이 곳에서 언급한 내용은 2006년도 연구보고서의 관련 내용을 최근 동향에 맞게 수정·보완한 것임

16) ISPS Code는 Part A와 Part B로 구분되어 있으며, Part A는 이행이 강제되는 사항을, Part B는 임의 규정으로 구성되어 있음.

17) 국제해사기구는 2002년 12월에 '1974년 국제인명안전협약(이하 "SOLAS협약"이라 함)' 개정을 위한 외교회의를 개최하였음. 이 회의에서는 SOLAS 협약을 개정, 제V장에 AIS(선박 자동 식별장치)의 조기 탑재를 의무화하고, SOLAS협약 제XI-1장 및 제XI-2장의 해상안전 및 보안특별조치를 신설하였음. 이 중 제XI-2장을 특별히 선박 및 항만시설의 보안에 관한 규칙이라고 지칭함.

18) 이 곳에서 언급하는 사항은 1974년 협약 개정안 가운데, 11-2장의 규정에 관한 강제요건(Part A)을 중심으로 하였음.

19) 이 규정의 적용대상선박은 고속 여객선을 포함한 여객선, 고속 화물선을 포함한 500톤 이상의 화물선, 그리고 이동식 석유 석유 시추 시설(mobile offshore drilling units) 등임.

는 수준에 불과하지만 선박보안 2단계와 3단계에서는 1단계보다 강화된 보안조치가 이루어지도록 설계되어야 한다.

둘째, 항만시설²⁰⁾에 대해서도 선박과 유사한 절차에 따라 보안계획을 수립·시행해야 한다. 항만시설 보안계획 역시 사전에 수행한 보안평가를 바탕으로 위험수준을 결정하고, 이에 적합한 단계별 보안계획을 작성해야 한다. 이 계획에는 항만시설의 운영에 위협을 줄 수 있는 무기류, 기타 모든 위험한 장치 등의 반입 및 사용을 통제할 수 있는 조치를 포함한다. 이 같은 항만시설 보안계획의 수립절차와 방식은 선박보안계획과 동일하나 선박의 보안과 연계, 운영된다는 점에서 차이가 있다. 이는 항만이 선박이 입·출항하는 물류의 결절점(node)이고, 선박의 입항여부에 따라 보안 취약성과 위험도가 각각 달라지는 특성에 따른 것이다. 이 같은 점을 고려하여 예컨대 항만보안 3단계에서는 화물의 적·양하 작업이 금지되는 것은 물론 선박의 운항이 전면 통제되고, 선박에 인가받지 않은 사람이 접근하는 것이 금지된다.

또한 ISPS 코드는 선박을 운항하는 선사에 대해서도 여러 가지 규정의 이행을 요구하고 있다. 이 같은 의무사항은 해당 선사가 해사보안문제에 대해 최종적으로 책임진다는 것을 전제로 한다.

첫째, 선사는 선박보안계획의 수립과 동시에 운항하는 선박마다 선박보안 담당관(ship security officer)과 회사보안 담당관(company security officer)을 임명해야 한다. 선박보안 담당관은 정기적으로 선박의 보안사항을 점검하고, 선박보안계획을 이행, 유지, 감독하는 권한과 책임이 있다. 이뿐만 아니다. 선박보안 담당관은 모든 보안사고에 대한 보고의무와 함께 항만시설 보안담당관과 당해 회사보안 담당관과 긴밀한 협력 체제를 유지하면서 선박보안계획을 이행한다. 회사보안 담당관은 적절한 보안평가와 기타 관련 정보를 활용하여 당해 선사에서 직면할 수 있는 위험수준에 대한 자문과 선박보안 평가업무를 수행한다.

둘째, 선사는 회사보안 담당관과 선장, 선박보안 담당관 등이 당해 업무를 수행하는데 필요한 지원을 해야 하는 것은 물론 주기적으로 교육과 훈련과정을 이수할 수 있도록 보장해야 한다.

한편, ISPS 코드를 포함하여 2003년에 동시에 채택된 1974년 SOLAS 협약 개정안을 협약 체결국에서 이행하는데 따른 행정적인 부담도 상당한 것으로 평가되고

20) 항만시설이란 선박과 항만 간의 연계가 이루어지는 곳으로 이 협약의 체결국에서 지정한 지역(위치)을 의미함.

있다.

첫째, 체약국은 선사나 항만 당국이 보안계획을 수립하는데 필요한 단계별 보안 수준을 결정해야 하고, 보안사고가 발생할 경우, 시설을 보호하는데 필요한 기본 지침을 제공할 의무가 있기 때문이다. 동시에 협약 체약국은 직접 또는 적절한 기관을 지정하여 선박 및 항만시설에 대한 보안계획을 승인해야 한다.

둘째, 선박 및 항만시설 보안계획의 승인과 관련하여 체약국 정부는 이 같은 업무를 수행하는 책임 있는 국가기관이나 지정된 기관이 있는 경우, 그 명칭과 상세한 연락처 등을 IMO에 제공하여 다른 체약국이나 선사 등에서 사용할 수 있게 해야 하는 부담도 있다.

셋째, 국제선박보안증서도 발행해야 한다. 이 증서는 협약의 적용을 받는 모든 선박을 대상으로 검사를 시행하고, 그 선박이 협약에서 정한 여러 규정을 준수하고 있는지를 판단하는 증거가 된다. 이 증서가 없으면 선박의 운항이 금지되기 때문에 관련 부처의 세심한 주의가 요청되고 있다.

넷째, 이 협약의 준수와 관련, 체약국은 항만국 통제(PSC : Port State Control)를 시행한다. 항만국 통제는 기존 협약에 정해진 바와 같은 방식으로 이루어진다. 따라서 이 협약에 가입하지 않은 국가의 선박에 대해서는 항만국 통제를 하지 않는다. 단, 가입국가의 선박보다 우월적인 대우를 할 수는 없다. 즉, 입항을 거절하거나 필요한 경우 억류 등의 조치를 취할 수 있다.

이 협약은 또 선박에 대한 보안을 강화하는 차원에서 몇 가지 제도적인 장치를 도입하고 있다. 선박식별번호의 부착과 선박 이력기록부의 작성을 의무화한 것이 이에 해당된다. 선박식별번호는 기존 IMO 번호를 선박에 영구적으로 표시하는 것으로 자동차 등록번호판을 선박에 다는 것과 같다. 다만 이 표지판은 선수부문이나 선체 양쪽 등 눈에 잘 띄는 곳에 부착해야 한다. 여객선인 경우에는 해면과 수평하게 표시해야 한다.

선박 이력기록부²¹⁾는 선박의 국적 변경이나 소유자의 변경현황 등을 손쉽게 확인하기 위한 장치이다. 따라서 선박을 소유한 해운회사의 명칭과 주소, 선박안전증서를 발행한 관할 기관, 선박을 검사한 해당 선급에 대한 명세를 기록한다. 이 같은 제도를 도입한 것은 선박이 ‘호적세탁’ 등과 같은 방법으로 국제테러집단에 이용되는 것을 막기 위한 조치로 풀이되고 있다.

21) Continuous Synopsis Record.

또한 선장에게는 선박의 안전과 보안을 유지하는데 필요한 폭넓은 권한이 부여된다. 예컨대 선장은 선박의 안전 등을 확보하기 위해 통관이 허용된 화물이라 하더라도 전문적인 견해에 따라 위험하다고 판단하는 경우에는 그 화물의 선적을 금지할 수 있고, 위험인물의 승선을 허용하지 않을 수 있다.

한편, IMO는 2006년 5월 해상안전위원회(MSC)에서 기존의 해상인명안전협약(SOLAS 1974/78) 제5장(항해 안전)을 개정하여 장거리 선박추적 시스템(LRIT)²²⁾의 도입을 의무화하였다. 이 제도 도입으로 300톤 이상의 모든 국제항해선박에 2008년 1월부터 이 같은 시스템을 선박에 탑재하고 운항해야 한다. 선박이 테러리스트 등에 탈취당하는 경우 신속하게 추적하고, 진압조치 등 필요한 조치를 취할 수 있는 방안이 마련된 것이다.²³⁾

2) 미국의 해운보안법

2002년 말 제정된 해운보안법(Public Law 107-295)²⁴⁾은 물류보안을 강화하는 미국의 입장과 시각이 그대로 반영된 법률이라 할 수 있다. 미국은 이 법률을 제정하면서 자국 해역을 운항하는 선박과 항만시설에 대한 보안조치를 강화하는 규정과 함께 외국항만에서 시행하고 있는 보안제도의 적정성을 평가하는 내용까지 포함했기 때문이다. 즉 미국 기준에 적합하지 않은 보안제도를 시행하는 국가의 항만에서 출항한 선박의 경우, 미국 항만에 입항하는데 일정한 제한을 가해 미국식 보안제도의 이행을 강제하겠다는 의도로 풀이된다. 이 같은 미국 해운보안법의 주요 내용을 살펴보면 다음과 같다.

첫째, 항만과 선박의 보안취약성 평가를 강제하고 있다. 이는 선박을 이용한 테러 등 운송보안사고²⁵⁾를 일으키기 쉬운 선박의 종류와 항만을 가려내기 위한 것이다. 미국 해운보안법은 매 5년마다 기초평가를 우선 시행한 다음 이를 토대로

22) Long Range Identification and Tracking System

23) 우리나라는 2007년 5월 12일 중국 발해 만에서 일어난 골든 로즈 호 침몰 등 최근 대형 해양사고가 잇따라 발생함에 따라 선박의 동정을 상시 파악할 수 있는 선박 위치 추적제(VMS : Vessel Monitoring System)를 도입, 시행하기로 했음. 즉, 선박안전법을 개정, 2007년 11월부터 모든 국제항행 선박에 VMS 제도를 도입하고, 국내항행 선박 중에서도 여객선, 유·도선, 낚시어선 등 다중 이용 선박에 우선적으로 시행하기로 했음.

24) Maritime Transportation Security Act of 2002

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

정밀평가를 시행하도록 요구하고 있다. 다만, 정밀평가를 시행하는 데 있어서는 항만시설에 대한 평가보다는 선박에 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 국토안보부 장관의 사전 승인을 받아야만 시행할 수 있으며, 중요사항이 변경될 때 역시 그러하다.

이 밖에도 이 법률은 해운보안사고에 대한 대응계획의 수립과 보안구역으로 지정된 곳의 출입을 통제하는 운송보안카드제도의 도입, 선박 자동식별 장치(AIS)의 설치를 의무화하고 있을 뿐 아니라 위성통신기술이나 조난선박구조 및 해상안전 시스템(GMDSS²⁶⁾)을 이용한 광대역 선박위치 추적시스템을 개발하고, 입항선박에 대해 적재하고 있는 화물의 정보를 사전에 신고하도록 규정하고 있다.

이 같은 규정은 2004년 7월부터 시행되고 있는 국제해사기구의 국제선박·항만 시설보안 규정(ISPS 코드)과 내용 면에서 큰 차이가 없다.²⁷⁾ 그러나 이 법률에서 명시하고 있는 외국항만에 대한 보안평가제도는 IMO 제도와는 전혀 다르다. 미국이 자체적으로 만들어낸 규정이기 때문이다. 이 법률에서 미국은 크게 3가지 점을 염두에 두고 있으나, 미국에 화물을 수출하는 외국항만의 보안상태를 직접 평가하겠다는 것이 핵심이다.

즉, 미국 해운보안법은 국토안보부 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 보안위험이 국제 해운 거래에 부담을 줄 것으로 우려되는 경우에도 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 자국 법률에 마련한 셈이다.²⁸⁾

26) Global Marine Distress and Safety System의 약자임.

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

28) 이와 함께 미국 해운보안법은 외국항만에 대한 보안평가를 크게 다음과 같은 6가지 기준에 따라 시행할 것을 규정하고 있음. i) 컨테이너 화물과 기타 일반화물, 그리고 수화물에 대한 검색이 올바르게 이

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 조치를 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 나서 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 입항금지, 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 국토안보부 장관에게 국무부장관과 협의 결과 해당 항만의 보안상태가 여객이나 선원 등이 이용하고, 선박이 입항하는데 위험을 준다고 판단한 경우에는 ‘90일 경과 기간과 관계없이 즉시 필요한 조치를 발동할 수 있도록 규정하고 있다.²⁹⁾

3) 운수근로자 신분증 제도

미국은 지난해부터 항만 근로자를 포함한 운수 근로자를 대상으로 신분증 발급제도를 도입하였다. 미국 국토안보부는 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.

루어지고 있는지 여부, ii) 화물·선박 및 부두 지역 등 출입통제지역에 대한 보안조치가 적절하게 이루어지고 있는지 여부, iii) 선박에 대해 적절한 보안조치가 이루어졌는지 여부, iv) 적절한 보안기준의 이행을 확인할 수 있는 증서나 서류 등이 갖추어졌는지 여부, v) 외국 항만의 보안관리 프로그램의 효율성, vi) 기타 미국에 대한 테러를 억제하는데 필요한 적절한 조치가 시행되고 있는지 여부 등임.

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

이 같은 조치는 최근 디피 월드의 미국 항만 터미널 인수 문제를 계기로 불거진 항만 보안을 강화하고, 불법 이민자들을 색출하기 위한 것으로 풀이되고 있다. 앞으로 3년 동안 추진하게 되는 ‘교통 근로자 신분 확인 및 증명서 발급 제도’³⁰⁾는 미국이 해운보안법에 따라 시행하고 있는 항만 근로자에 대한 범죄 경력조회제도를 보완하는 것으로 해석되고 있다.³¹⁾

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 시행하는데 앞으로 10년 동안 2억 9,000만 달러에서 3억 2,500만 달러가 소요될 것으로 추정하고 있어 비용이 부담된다는 점이다. 또한 항만 근로자의 경우 신분증을 발급받는데 1인당 109달러의 발급 수수료를 내야 하는 부담도 있다. 미국 전체적으로는 10억 달러 이상의 비용이 들어가는 것으로 전문가들은 분석하고 있다.

둘째, 신원 조사 과정에서 상당수의 운수 근로자들이 신분증 발급을 거절당할 가능성이 크다는 점이다. 미국 국토안보부는 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.³²⁾ 특히 컨테이너 트럭 운송업체의 경우 멕시코계 무자격 기사가 많아 향후 결과 여하에 따라 인력 부족 현상이 심화될 가능성도 배제할 수 없다는 주장도 제기되고 있다.³³⁾

30) the US Transportation Workers Identification Credential Programme

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

32) *Fairplay*, 2006. 6. 8

33) 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, 프레이저 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).

2. 컨테이너화물 검색제도

1) 컨테이너 보안 대책(CSI)

컨테이너 화물 검색제도도 물류보안을 확보하는 수단의 하나다. 미국은 컨테이너 내에 테러 등에 악용될 수 있는 위험한 물질이 들어 있는지 확인하기 위해 2002년 1월에 컨테이너 보안 대책(CSI : Container Security Initiative)을 도입하였다. 즉, 이 제도는 외국에서 대량살상무기(WMD) 등이 선박을 통해 자국으로 밀반입되는 것을 차단하는데 역점을 두고 있다.

이 제도는 외국의 항만에서 해당국 세관이 미 세관원과 공동으로 미국행 컨테이너 화물을 선적하기 24시간 전에 화물 투시기(X-ray)나 방사능 탐지기 등으로 위험화물을 사전 검색하여 적발하는 것을 핵심으로 하고 있다. 미국은 이 제도를 통해 자국으로 반입되는 연간 570만 개의 컨테이너 화물 가운데 적어도 2% 정도를 검사하여 위험성이 높은 화물의 반입을 사전에 차단한다는 방침이다.

이 제도는 위험성이 높은 컨테이너 화물의 반입을 통제하는 수단의 하나로 관세·국경보호청(CBP)의 주도 하에 미국과 개별국가 간에 양자협정을 체결하여 시행하고 있다. 미국은 이 제도를 미국 수출 컨테이너 화물의 68%를 점유하고 있는 세계 20대 대형 항만(mega ports)에 우선 적용하는 한편, 그 적용 대상 범위를 더욱 확대하고 있다. 2007년 5월 현재 미국과 CSI 협정을 체결한 항만은 독일, 네덜란드, 싱가포르, 홍콩, 일본 등에 50곳이 넘고 있다. 우리나라 또한 미국과 이 협정을 체결하여 부산항에서 미국행 컨테이너 화물에 대한 검색을 실시하고 있다.

2) 미 항만보안법의 시범 사업

한편, 미국이 2006년 10월에 이른바 항만보안법(SAFE Port Act)을 제정하면서 컨테이너 화물 검색제도가 크게 변할 양상을 보이고 있다. 양자협정으로 이뤄지던 이 제도를 법률에 포함시키는 한편, 화물의 검색 비율을 100%로 높이는 시범사업(pilot project)을 진행하도록 규정하고 있기 때문이다. 미국 국토안보부는 이 법률이 시행됨에 따라 2006년 말에 시범사업을 진행할 외국의 6개 항만을 선정하였다. 지난해 10월 13일 제정된 미국 항만보안법은 법률이 공포된 이후 90일 이내에 외국의 항만 3곳을 선정해 시범사업을 진행하도록 규정하고 있다. 시범사업 대상항

만으로 선정된 곳은 지역적으로 각 대륙에 균등하게 분포하고 있다. 아시아권에서는 홍콩을 제외하고, 우리나라와 싱가포르 등 2곳이 포함된 것이 특이하다는 분석도 나왔다.³⁴⁾

<표 2-1>

시범사업 대상 항만

항만	부산항 감만 터미널	카심	사우스 햄튼	싱가포르	살라라	푸에르토 코르테스	모던 터미널
국가	한국	파키스탄	영국	싱가포르	오만	온두라스	홍콩
운영	허치슨	디피 월드	디피월드	PSA	APM	Empresa Nacional Portuaria	모던 터미널 주식회사

주 : 최근 홍콩의 모던 터미널이 검색 시범대상 항만으로 추가됐음.

자료 : 한국해양수산개발원.

미국은 선정된 일부 항만(터미널)에서 2007년 상반기부터 시범사업에 착수하였다. 영국의 사우스햄튼 항만, 파키스탄의 카심 항만 등 3곳이 우선 시범사업에 들어갔다. 나머지 3개 항만은 검색시스템 설치 등 여전히 성숙되는 대로 검색을 실시한다는 방침이다. 시행 초기에는 미국 수출 컨테이너를 7% 이상 검색하다가 2007년 말에는 100%까지 검색 비율을 확대한다는 방침이다. 지금까지 외국 항만에서 미국 수출화물에 대한 검색 비율은 통상 1%를 밑돌았으며, 우리나라의 경우는 하루에 1~3개에 지나지 않았다.

미국은 항만보안법을 제정할 당시 미국으로 수출되는 모든 컨테이너 화물에 대한 검색을 추진하였다. 그러나 관련업계의 강력한 반대에 직면, 시범사업을 실시한 뒤 사업 확대를 추가로 검토하기로 하였다. 미국 국토안보부 체토프 장관은 외국 정부와 터미널 운영업체와의 협력을 통해 이 사업을 가능한 한 빨리 확대할 방침이라고 밝힌 바 있다. 당초 시범사업 대상항만이 3곳에서 7곳으로 늘어난 것도 미국의 이 같은 정책에 따른 것으로 풀이되고 있다.³⁵⁾

34) 미국은 시범사업을 시행하기 위해 2007년 2월부터 우리나라 부산항에서 시범사업에 대한 설명회를 개최해오고 있음.

35) 최근 홍콩 항만의 모던 컨테이너 터미널이 미국행 컨테이너 화물의 100% 사전 검색 시범사업이 참여하기로 함에 따라 이 프로그램에 참여하는 항만은 모두 7개로 늘어났음.

3) 수입 컨테이너 100% 검색 의무화

미국은 그 동안 논란이 많았던 수입 컨테이너 화물에 대한 100% 사전 검색을 의무화하였다. 미 의회는 지난 7월 27일 상하 양원에서 각각 심의해온 ‘9·11 테러 대책 위원회 권고 이행법률’의 조문 수정작업을 마무리하고, 법률로 시행하기 위해 백악관에 법안을 이송하였다. 조지 부시 대통령은 업계의 예상을 깨고, 이 법안에 전격적으로 서명하였다. 이 법률은 선박을 이용해 컨테이너 화물을 미국에 수출하는 경우 5년 이내에 외국에서 전량 사전 검색을 의무화하는 내용을 담고 있다. 또한 이 법률은 사전 검색이 이뤄지지 않은 컨테이너 화물에 대해서는 미국으로 반입할 수 없도록 규정하고 있다.

이 법률이 제정되기 전 2006년 11월 중간 선거에서 상·하 양원을 장악한 미국 민주당은 수입하는 모든 컨테이너 화물에 대해 100% 사전 검색을 의무화하는 법안을 제출하는 등 연초부터 강력한 보안 드라이브 정책을 추진해 왔다. 미 민주당은 2001년 9·11 테러 이후 조사위원회가 권고한 자국 보안조치 개선 방안을 입법화하는 과정에서 법안에 이 같은 내용을 포함하였다. 또한 민주당은 2006년 10월 항만보안법을 제정하다가 손을 대지 못한 내륙운송 및 철도 보안에 관한 내용도 이 법률에 대폭 반영하였다.

미국이 새로운 법률을 제정한 것은 지난해 10월부터 시행에 들어간 이른바 항만보안법의 내용을 더욱 강화하는 것으로 해석되고 있다. 항만보안법에서는 외국 의 주요 항만을 선정(7개 항만 이미 선정)해 시범 사업을 시행한 뒤 그 결과를 보고 100% 사전 검색 여부를 결정하도록 규정하고 있기 때문이다.

미국 수출 컨테이너 화물에 대한 사전 검색문제는 컨테이너 보안 협정(CSI) 제도가 도입된 이후 국제적으로 많은 논란을 불러일으키고 있는 사안이다. 미국은 자국으로 밀반입되는 대량살상무기를 차단하기 위해서는 어쩔 수 없다는 입장을 고수하고 있다. 전문가들은 미 민주당이 2008년 대통령 선거를 겨냥, 공화당과의 차별성을 부각하기 위해 물류부문의 보안조치를 앞으로 더욱 강화할 것이라는 분석도 내놓고 있다.³⁶⁾

36) 이 법안이 선사와 화주들의 강력한 반발에도 불구하고 입법화될 경우, 우리나라 모든 항만에 컨테이너 화물 검색기를 설치해야 할 뿐만 아니라 그로 인해 항만에서 화물 처리 지연 등 물류 왜곡현상이 일어날 가능성도 있으므로 입법 추이를 지속적으로 관찰할 필요가 있음.

4) 화물정보 24시간 전 신고제도

미국으로 수출하는 컨테이너 화물에 대한 정보를 사전에 신고하도록 하는 제도도 컨테이너 화물의 검색과 관련하여 중요한 기능을 하고 있다. 미 관세청은 컨테이너 보안 대책(CSI)을 도입하면서 이 제도도 동시에 도입하였다. 즉, 화물을 미국으로 수출하는 모든 운송인에게 화물을 선박에 적재하기 24시간 전에 적하목록(manifest)을 미 관세청의 자동 적하목록 시스템(Automated Manifest System : AMS)에 신고하도록 하고 있다.

이 제도는 현행 컨테이너 보안 대책(CSI)을 보완하는 기능을 하고 있다. 즉, i) 외국 항만에 파견되어 있는 미국 세관원에게 검사대상화물에 대한 정보를 즉시 제공하는 효과 외에 ii) 외국 항만에서 시행된 컨테이너 보안 검사에서 적발되지 않은 미국행 화물을 미국 항만에서 다시 검사할 수 있는 이중 검색 수단으로 활용하기 위해 마련된 제도이기 때문이다.

미국은 이 제도의 이행을 강제하기 위해 규정을 위반하는 경우 선장에게 첫 위반에 대해서는 5,000 달러, 그 이후의 위반에 대해서는 위반 시마다 1만 달러의 벌금과 함께 선박을 억류하거나 몰수하도록 하는 처벌 규정도 두고 있다.

3. 물류보안 인증제도

물류보안 인증제도 도입이 보편화되고 있다. 미국이 반테러 민·관 협력제도(C-T PAT)³⁷⁾를 2002년 4월부터 시행한 이후 세계관세기구(WCO)와 국제표준기구(ISO) 등 유사한 제도³⁸⁾를 각각 도입하고 있기 때문이다. 또한 유럽연합(EU)도 WCO의 제도를 수용한 이른바 기업 물류보안 인증제도(AEO)³⁹⁾를 2008년부터 본격적으로 시행할 계획이다.⁴⁰⁾ 이 밖에도 싱가포르는 2007년 5월 25일 민간기업을 대상으로 하는 물류보안 인증제도(STP)⁴¹⁾를 내놨다.⁴²⁾

37) Customs-Trade Partnership Against Terrorism의 약자임.

38) WCO는 2005년 10월에 「국제교역의 안전과 간소화를 위한 국제기준(Framework of Standard to Secure and Facilitate Global Trade)」을 채택하고, 2007년부터 단계적으로 시행할 계획임.

39) Authorized Economic Operator의 약자임.

40) 유럽연합은 2006년 12월 18일 기존의 관세청 규칙을 개정한 새로운 물류보안규칙(Commission Regulation 1875/2006)을 채택했음. 이 규칙에서 EU는 2008년 1월부터 AEO 제도를 도입하고, 2009년 7월부터는 교역업자와 세관 사이에 모든 수출입화물에 대한 정보(manifest)를 사전에 전자적인 방법으로 신고(교환)하도록 했음. 또한 EU는 회원국 사이에도 화물 정보를 교환하기로 했는데, EU의 이 같은 제도는 WCO의 SAFE Framework와 기본적으로 같은 개념임.

<표 2-2>

주요국의 물류보안 인증제도

국가별	제도 명칭	시행일
미국	반테러 민·관 협력제도(C-T PAT)	2002년 4월
유럽연합(EU)	기업 물류보안 인증제도(AEO)	2008년 1월
싱가포르	안전한 교역 협력 프로그램(STP)	2007년 5월
세계관세기구(WCO)	국제 교역의 안전과 간소화를 위한 국제기준(SAFE Framework)	2006년 8월
국제표준기구(ISO)	ISP/PAS 28000	2005년 5월

자료 : 한국해양수산개발원

물류보안 인증제도는 물류 전 구간의 보안을 확보하기 위해 일정한 요건을 충족한 사업자(기업)에 대해 보안활동을 충실하게 이행하고 있다는 자격을 부여하는 것을 핵심으로 하고 있다. 또한 인증받은 기업에 대해서는 화물을 수출입하는 과정에서 검사 횟수를 줄여주거나 통관 검사 자체를 생략하는 등의 혜택을 부여하고 있다. 민간기업의 참여를 권장하기 위한 일종의 유인책이다.

1) 물류보안 인증 대상기업

물류보안 인증제도에 따라 인증을 받을 수 있는 기업, 즉 적용 대상 기업은 나라마다 약간씩 차이가 있다. 이 제도를 처음으로 도입한 미국의 경우는 대상 기업을 6개 업종으로 한정하고 있다. 즉, 미국의 수입업자, 선사 및 항공사, 항만·터미널 운영업체, 도로운송사업자, 혼재업자, 포워딩 업체(화물운송 주선업자), 통관중개업자와 일부 외국의 제조업체만이 C-T PAT에 가입할 수 있다. 여기서 외국의 일부 제조업체란 미국과 국경을 맞대고 있는 캐나다와 멕시코의 제조업체를 의미한다. 미국이 C-T PAT를 기본적으로 자국 기업에 대해 적용하면서 일부 외국기업에 가입을 허용하고 있는 것은 이들 국가와 북미자유무역협정(NAFTA)을 체결하고 있고, 자동차 등으로 화물이 신속하게 이동하기 때문이다.

이에 비해 유럽연합이나 싱가포르, WCO 및 ISO 등은 물류보안 인증기업을 제한하지 않는 것이 특징이다. 즉, 유럽연합은 AEO 제도에 참여할 수 있는 대상으로 업무와 관련해 세관의 규칙이 적용되는 모든 기업(사람)이라고 규정하고 있다. 내

41) Secure Trade Partnership Programme의 약자임.

42) 싱가포르는 이 제도를 도입하기 전에 APL, IBM 싱가포르, UPS 싱가포르 등 8개 기업을 대상으로 시범사업을 성공리에 수행했다고 밝혔음(2007년 5월 25일, 싱가포르 보도자료).

용 면에서는 미국에 비해 문호가 크게 개방되어 있는 것으로 보인다. 다만, 2007년 5월 7일 유럽연합이 발간한 ‘기업 물류보안 인증제도 지침’⁴³⁾에 따르면, 해외 제조업체 등에 대한 별도 규정이 없다. 이것은 AEO 제도가 EU 역내 회원국에 대해서만 적용된다는 의미로 해석된다. EU 역외에서 활동하는 기업의 물류보안 인증은 WCO에서 제정한 SAFE Framework에 따라 국가간 상호 인증으로 해결하면 되기 때문이다.

<표 2-3>

물류보안 인증제도 적용 대상

제도 명칭	적용(가입) 대상 기업
반테러 민·관 협력제도(C-T PAT)	미국 수입업자 등 6개 업체
기업 물류보안 인증제도(AEO)	세관 규칙이 적용되는 모든 기업
안전한 교역 협력 프로그램(STP)	싱가포르의 물류 활동 종사기업
국제 교역의 안전과 간소화를 위한 국제기준	물품의 국제간 이동에 종사하는 모든 당사자
ISP/PAS 28000	물류활동에 참여하는 모든 조직

자료 : 한국해양수산개발원

WCO의 SAFE Framework에서는 “물품(goods)의 국제간 이동에 종사하는 모든 당사자”로 규정하고 있어 그 적용 범위가 매우 포괄적이다. 비교적 최근에 마련된 싱가포르의 안전한 교역 협력 프로그램(STP)은 싱가포르에서 물류 활동에 종사하는 모든 기업을 적용대상으로 한다. 그러나 이 같은 규정에도 불구하고 실제로 STP에 따라 인증을 받을 수 있는 기업은 미국의 C-T PAT과 큰 차이가 없을 것으로 보인다.

한편 ISO⁴⁴⁾ 28000⁴⁵⁾은 기업의 규모와 상관없이 모든 조직이 운영하고 있는 물

43) Authorized Economic Operator Guidelines.

44) 국제표준기구(ISO)에서 물류보안과 관련하여 현재 진행하고 있는 국제규범 제정 작업은 컨테이너 전자 봉인(E-seal)에 관한 국제표준과 이 곳에서 언급하고 있는 기업의 물류보안관리 표준과 인증에 관한 기준 제정 등 2가지로 대별됨.

45) ISO 28000이 국제표준으로 공식 결정되기 전에 이 문서는 PAS(Publicly Available Specification)를 붙여서 사용했는데, PAS란 ISO의 전문가들이 모인 위원회에서 잠정적으로 합의한 협약으로서 회원국의 50% 이상이 동의하면 발표됨. 그 후 3년 후에 재검토 과정을 거친 후 국제 표준안으로 확정할 것이지를 결정함. 따라서 물류보안관리 시스템을 위한 표준안인 ISO/PAS 28000은 2005년 11월 15일에 발표되었으므로 3년 후인 2008년 11월 15일 이후에 국제 표준으로 최종 확정될지 여부를 결정하게 됨. ISO는 2008년 11월 28일에 이를 국제표준으로 최종적으로 확정했음.

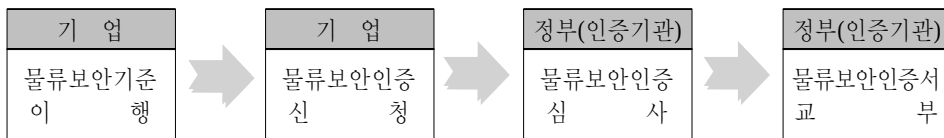
류 전 과정, 즉 제조, 서비스, 보관·운송 전 분야에 적용이 가능한 것이 특징이다. 이 같은 점이 자국 내 기업에 한해 인증을 부여하는 유럽연합이나 미국의 물류보안 인증제도와 다르다. ISO/PAS 28000이 사업장 물류보안 인증에 관한 국제표준이라는 데서 오는 차이라고 이해하면 된다.

2) 인증 요건 및 인증 절차

미국의 제도 또는 국제기구 협약 중 어느 것을 따르던지 기업이 물류보안에 관한 인증을 받는 절차는 대동소이하다. 기업이 일정한 물류보안 요건을 충족(이행)하고, 인증신청서를 제출하면, 일정한 심사과정을 거쳐 자격이 있는 것으로 판단되는 경우 최종적으로 물류보안 인증서를 발급하는 것이 각국이 채택하고 있는 일반적인 물류보안 인증절차이기 때문이다. 이 같은 과정을 유럽연합을 예로 들어 설명하면 다음과 같다.

<그림 2-1>

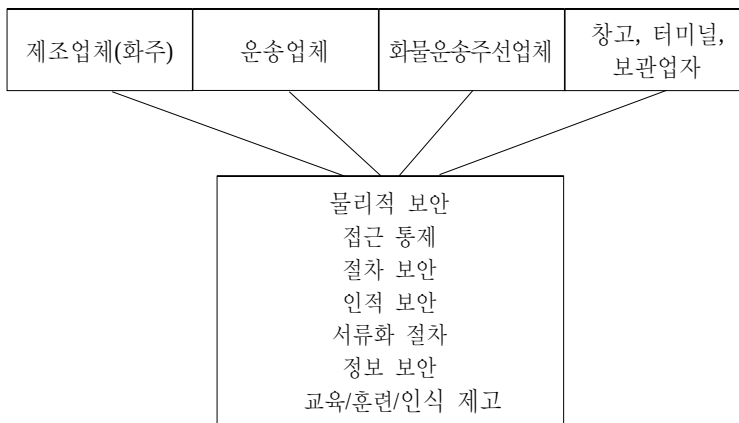
물류보안 인증 절차



자료 : 한국해양수산개발원

<그림 2-2>

물류보안 인증에 필요한 최소 기준(EU)



자료 : 한국해양수산개발원

<표 2-4>

운송인 물류보안 인증 특별요건(EU)

항목	특별요건
물리적 보안	- 모든 건물과 재산이 불법진입·침입으로부터 보호될 것 - 다음 사항을 포함 •내·외부 문, 창문, 담장 등의 잠금장치 •내부 및 주차장을 포함한 외부 시설의 조명 •개인차량의 주차지역을 양·적하 및 화물지역과 분리 •내외부 통신시스템을 내부 보안인력 또는 지역 공안들과 연결
출입 통제	- 시설 및 운송수단에 대한 불법 접근 금지 - 통제는 다음사항을 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, 불법적인 물질접근을 막기에 적합할 것 - 보안절차는 다음을 포함해야 함 •화물 및 화물장비의 고유표식, 수량 파악 및 기록(문서 작성) •화물이 반입될 때 화물의 봉인 무결성 또는 다른 보안장치의 통제 •화물 이동시 봉인 및 다른 보안장치 확인 절차 •감시시스템 및 부족 보고 •반입, 반출 화물의 이동 및 운송수단의 추적 •불법적 접근을 막기 위한 공개 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 - 보안 사건에 대한 보고 절차가 적합할 것
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
서류화 절차	회사는 서류의 완결성, 판독성, 정확성 및 제출 시간을 확인
정보 보안	물류 부문에서 정보전달 절차를 확실하게 유지
안전한 화물흐름 조항 (Secure freight flow provisions)	- 회사는 승인된 운영자가 아닌 운영자가 제공한 화물을 엄격하게 검사하여 승인된 운영자의 화물 수준으로 향상시켜야 함 - 만약 검사가 시행되지 않거나 화물이 승인된 공급망의 “신속 조치” 부분의 화물로 판단되지 않는다면 거절

자료 : 유럽연합(EU)

첫째, 물류보안 인증을 받고자 하는 기업은 사업장(회사)의 물리적 보안 등 최소한 7개 항목의 기준을 충족하고 있어야 한다. 또한 이 같은 기준을 이행하기 전에 기업은 자체 사업장 등의 보안상태에 대한 위험평가(risk assesment)를 실시하고, 필요한 대응조치를 정해진 규정에 따라 마련해야 한다. 미국의 C-T PAT나 유럽연합의 AEO 제도 등에는 업종별로 물류보안 인증에 필요한 최소한의 요건 등에 대해 규정하고 있다.⁴⁶⁾

둘째, 물류보안 인증을 받고자 하는 기업은 일정한 서식에 따라 작성된 문서를 인증기관(정부)에 제출하여야 한다.⁴⁷⁾ 미국의 경우는 인증 심사를 간소화하기 위해 별도의 인터넷 포털 사이트를 구축·운영하고 있다. 즉, 인터넷 홈페이지를 통해서만 인증심사를 신청할 수 있다.

<표 2-5>

물류보안 인증기관

제도 명칭	인증 심사기관
반테러 민·관 협력제도(C-T PAT)	세관·국경보호국(CBP)
기업 물류보안 인증제도(AEO)	유럽연합(EU) 회원국에서 결정
안전한 교역 협력 프로그램(STP)	싱가포르 관세청
국제 교역의 안전과 간소화를 위한 국제기준	회원국 세관 당국
ISO 28000	선급협회

자료 : 한국해양수산개발원

여기서 인증업무를 담당하는 기관으로는 대체적으로 세관당국(관세청)이 참여하고 있다. 미국의 경우 세관·국경보호청(CBP)에서 C-T PAT 업무를 처리하고 있고, WCO의 SAFE Framework은 세관 당국을 AEO 업무 담당기관으로 특정하고 있다. 유럽연합의 경우는 회원국에 대해 AEO를 담당하는 기관을 정하도록 규정하고 있다. ISO의 물류보안 인증업무는 대체적으로 선급기관에서 수행하고 있다.

46) 2007년 5월 25일 민간기업 물류보안 인증 기준(STP)을 발표한 싱가포르는 이와 약간 다른 기준을 제시하고 있음. 즉, 시설 보안 및 접근 통제, 인적 보안, 비즈니스 파트너 보안, 화물 보안, 운송보안, 정보 및 정보 기술(IT) 보안, 보안사고 관리 및 조사, 위기관리 및 사고 복구 등을 이행기준으로 삼고 있음.

47) 물류보안 인증을 신청할 때는 각국이 작성한 신청서와 함께 해당 기업에 대한 소개, 회사의 보안 관련 자료(profile)-회사 보안관리시스템 요약, 회사의 위험 평가절차 개요, 당해 회사의 물류보안을 강화하기 위해 회사가 마련한 보안 조치 등-회사의 물류활동에 수반되는 화물 및 정보 흐름을 표시한 절차도와 회사의 물리적 보안을 확보하는 방안이 표시된 계획서 등을 포함한 문서, 기타 회사의 보안 관련 증서와 기타 보안활동을 입증할 수 있는 문서 등을 제출해야 함.

3) 인증 기업에 대한 혜택

물류보안 인증업무는 현재 자발적으로 시행되고 있다. 따라서 물류기업의 참여를 높이기 위해서는 일정한 혜택을 부여하는 것이 필요하다. 이와 관련해 국가마다 약간의 차이는 있지만, 크게 두 가지 혜택이 있는 것으로 입장을 정리하고 있다.

첫째, 물류보안을 강화함에 따라 기본적으로 물류 전 구간에서 화물의 가시성(visibility of goods)을 향상시킬 수 있다. 또한 화물의 도난을 방지하는 등 물류 관리의 효율성을 높일 수 있다는 것이 가장 큰 장점으로 부각되고 있다.

둘째, 기업이 물류보안 인증을 받는 경우 세관을 이용하는데 따른 일정한 혜택도 부여된다. 미국의 세관·국경보호국(CBP)은 이와 관련해 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

미국에서 부여하는 이 같은 혜택은 다른 나라에서도 거의 비슷하다. 유럽연합은 회원국 중 한 국가에서 기업이 물류보안 인증을 받으면, 그 지위는 다른 회원국에서도 인정되도록 했다. 또한 물류보안 인증 기업은 역내 회원국에 보안통제 조치를 편리하고 간편하게 받을 수 있다(fast track treatment : 우선 처리 혜택). 여기서 편리하고 간편하게 보안통제조치를 받는다는 것은 인증을 받지 않은 기업과는 다른 화물 통과나 절차를 받을 수 있는 것을 의미한다. 싱가포르도 STP 프로그램에 따라 물류보안 인증을 받을 기업에 대해서는 i) 화물의 검사 횟수를 줄여주고, ii) 안전한 기업(예)이라는 브랜드를 사용하도록 인정하는 한편, iii) 통관 절차의 간소화와 iv) 다른 나라와의 상호 인증협정을 통해 물류보안 인증 지위를 인정해주기로 하였다.

<표 2-6> 주요국의 물류보안 인증프로그램

	미국	EU	WCO	일본
프로그램	C-T PAT	EU세관법 및 시행규칙	국제무역의 안전 확보 및 원활화를 위한 「규준의 범위」	적하(積荷), 여객 및 승무원에 관한 사항의 사전보고제도
관할기관	미국세관(CBP)	EU가맹국세관	WCO 가맹국세관	재무성관세국
프로그램의 법제화	CBP와 민간 임의 프로그램	2005년 4월13일 제정개정관세법, 2006년 12월 18일 제정 개정시행규칙	2005년 6월23일 WCO총회에서 「규준의 범위」가 채택, 묵하 계속심의 중	관세법, 관세법시행령
대상	수입	수입 및 수출	수입 및 수출	수입
대상기업	미국의 수입자, 캐리어, 포워더, NVOCC, 특정외국 기업, 브로커	AEO(통관에 관련한 업무를 실시하는 서플라이체인 기업, 자)	AEO(기업, 수출입자, 캐리어, 브로커, 오퍼레이터 등)	선회사, 항공회사, 혼재업자(예정)
목적	▶ 세관은 모든 수입화물을 검사할 의의책임이 있다. ▶ C-T PAT는 수입, 수출 등 미국으로의 수입화물에 직접적으로 책임 임을 부담하고, 벌을 준수하는 Raw-risk 기업의 참가를 요구.	▶ 지금까지 개별적으로 간이토포관 수속을 인정해 왔다. ▶ EU레벨로 제도를 일반화하고, 보안을 위한 필요요건을 지키는 기업에게는 AEO의 지위를 부여	▶ 글로벌한 레벨에서 서플라이체인 안전 확보 및 원활화에 이어 규정된 규준을 정한다 ▶ 모든 수출수단에 대하여 통합된 SCM을 가능하게 한다.	일본의 테러행위와 국제적인 범죄 조사를 미연에 방지하기 위해
요건	▶ 거래관계처 요건 보안수속 등 ▶ 내부규준 컨테이너 • 보안등	▶ 적절한 compliance 기록 ▶ 상업과 수출에 관계된 기록의 관리 ▶ 재무적 건전성의 증명 ▶ 보안과 안전기준	▶ 세관요건의 준수 ▶ 상업기록의 관리 ▶ 재무의 건전성 ▶ 화물의 보안 등	
배네핏	▶ 검사회수를 적게한다 ▶ 우선적으로 검사를 실시	▶ 관세규칙에 기반한 통관간소화의 보완과 안전에 관계된 세관관리	▶ 화물의 양도를 촉진하는 수단, 수출시간의 삭감과 보관 비용의 저감	
화물 정보의 사전통지	▶ 해운컨테이너화물 수입·외국항에서 석적의 24시간전 수출·미국직항 출항 24시간전 ▶ 항공화물(장거리비행) 수입·미국도착 4시간전 수출·미국출발 2시간전	▶ 해운컨테이너화물 수입·출발항에서 석적의 24시간전 수출·EU출항본선으로의 신적24시간전 ▶ 항공화물(장거리비행) 수입·EU도착 4시간전 수출·EU출발30분전	▶ 해운화물 수입입항하기 24시간전까지 보고 근거 없는 입항 12시간전 또는 입항전 ▶ 항공화물 항공운송시간 5시간이사아-입항3시간전 3시간전~5시간미만-입항1시간전 3시간미만-입항하기까지	

출처 : 「서플라이체인 • 보안 • 프로그램의 국제비교」 일본기계수출조합, 2006년 6월, 11~16항에 기반하여 필자작성.

제3장 우리나라 물류보안제도 현황과 문제점

1. 우리나라 물류보안제도 현황

우리나라에서 물류보안업무와 직접적으로 관련된 부처는 해양수산부와 건설교통부라 할 수 있다. 그리고 국가정보원과 관세청, 외교통상부, 산업자원부 등도 일정부분 물류보안업무와 연관되어 있다. 이 가운데, 해양수산부는 주로 항만과 선박을 중심으로 하는 물류부문의 보안업무를 담당한다. 건설교통부는 내륙 교통 및 항공부문의 보안업무 주 수행기관이다.

우리나라는 남북이 대치하고 있는 특수상황 때문에 다른 나라에 비해 국가 중요시설에 대한 보안조치는 비교적 양호한 것으로 평가되고 있는 것이 사실이다. 통합 방위법에 따라 국가 중요시설의 소유자 또는 관리자에 대해 경비·보안책임을 지도록 하고, 통합방위사태에 대비하여 자체방호계획을 수립하도록 요구하고 있기 때문이다.

<표 3-1>

부처별 주요 물류보안제도 현황

부처 별	주요 제도
해양수산부	1. ISPS 코드 등 IMO 보안협약 시행 2. ISPS 코드 이행법률 입법 추진 3. 컨테이너 100% 검색 시범사업 추진
건설교통부	1. 항공안전 및 보안에 관한 법률 시행 2. 상용화주제도
관 세 청	1. 미국과 컨테이너 보안협정(CSI) 체결 2. 벨기에와 컨테이너 화물 추적 시범사업 시행합의
국가정보원	1. 물류보안체제 구축 민관 협의체 구성·운영 등

자료 : 한국해양수산개발원

그러나 통합 방위법은 적의 남침 등에 대비해 시설에 대한 방호를 염두에 두고 제정한 법률이기 때문에 물류보안 측면에서는 원용할 수 있는 규정이 많지 않다는 점에 유의할 필요가 있다.⁴⁸⁾

정부 부처별로 담당업무와 2001년 9·11 테러 이후 지금까지 마련하거나 또는

새로 도입한 주요 물류보안제도의 시행 현황을 정리하면 <표 3-1>과 같다.

1) 해양수산부

해양수산부는 국제해사기구(IMO)에서 제정한 ISPS 코드를 직접 이행하는 등 물류보안업무를 수행하고 있다. 첫째, 2004년 7월 1일부터 국제항해에 종사하는 선박과 28개 무역항을 중심으로 ISPS 코드를 시행하고 있다. 해양수산부는 이 제도 도입에 앞서 고시를 제정, ISPS 코드의 국내 시행에 필요한 절차 등을 마련하였다. 국제 항해 선박 및 항만시설의 보안에 관한 규칙이 그것이다.

둘째, 이와 함께 해양수산부는 지금까지 고시형태로 시행하고 있던 ISPS 코드를 수용하는 법률을 2007년 8월에 제정하였다. 해양수산부는 2006년에 이 법률의 조문 작업을 매듭짓고, 필요한 입법절차를 거쳐 국회에 제출한 바 있다. 이에 따라 가칭 ‘국제 항해선박 및 항만시설의 보안에 관한 법률’이 2007년 하반기부터 시행되고 있다. 다만, 이 법률을 제정하는 과정에서 논란을 빚었던 항만시설 보안료 징수와 관련된 규정은 법률 시행일부터 3년간 유예하는 것으로 합의되었다.

해양수산부가 ISPS 코드를 시행할 수 있는 고시가 있음에도 불구하고, 별도 법률을 제정한 나선 것은 그 동안 고시시행 과정에서 제시됐던 몇 가지 사항을 보완하고, 보다 완벽한 법적 시스템을 구축하기 위한 것이다. 특히 이 법률은 두 가지 점에서 고시 내용과 크게 차이가 있다.

첫째, 국가 항만보안계획을 수립하도록 하였다. 해양수산부장관은 선박 및 항만시설의 보안에 관한 업무를 효율적으로 수행하기 위하여 항만보안의 기본방침 또는 보안사건의 대비·대응조치 등을 주요 내용으로 하는 국가항만보안계획을 10년마다 수립·시행하도록 하고, 지방해양수산청장은 국가항만보안계획에 따라 관할구역의 항만시설에 대한 지역항만보안계획을 수립·시행하도록 이 법률안은 명시하고 있다.

둘째, 항만시설 보안료를 부과할 수 있는 근거를 마련하였다. 이 법률은 항만시설 소유자에 대해 당해 항만의 보안을 확보하는데 필요한 여러 가지 의무를 부과하고 있다. 이 같은 의무와 관련해 이 법률은 제42조에서 항만시설소유자에 대해 “제22조에 따른 국제항해여객선에 대한 보안검색과 제31조에 따른 경비·검색 인력 및 보안시설·장비의 확보 등에 소요되는 비용(이하 “항만시설 보안

48) 한국해양수산개발원, 「국가물류보안체계 확립방안 연구(I)」, 2006. 12, p. 10.

료”라 한다)을 당해 항만시설을 이용하는 자로부터 징수할 수 있다”고 규정하고 있다.

한편, 미국 수출 컨테이너 화물에 대한 100% 사전 검색시범 사업도 추진하고 있다. 우리나라 부산항의 감만 터미널은 미국 항만보안법에서 규정한 이른바 컨테이너 100% 사전 검색 시범 사업 대상 항만으로 선정되었다. 이에 허치슨 터미널이 운영하는 감만터미널에서 2007년 10월 13일까지 시범 사업에 필요한 검색 장비를 설치하고, 미국행 컨테이너 화물에 대한 검색 작업에 착수해야 한다.⁴⁹⁾ 미국은 이 같은 사업을 진행하면서 부산항의 미국행 컨테이너 물동량이 많은 점을 고려해 검색 비율을 탄력적으로 조정한다는 방침이다. 즉, 시행초기에는 게이트 혼잡현상이 발생할 우려가 있다고 보고, 검색 비율을 낮게 한 다음 운영 상황을 고려, 그 비율을 점차적으로 상향조정한다는 것이다. 미국의 이 같은 방침은 시범 사업대상 항만으로 지정된 항만 가운데, 미국행 컨테이너 물동량이 많은 영국의 사우스햄튼 항만이나 싱가포르 항만에도 적용되는 것으로 알려졌다.

2) 건설교통부

건설교통부는 육상 부문과 항공 부문의 물류보안을 담당하는 정부부처다. 산하에 항공안전본부(항공보안과)를 설치, 항공부문에 대한 보안업무를 전담하게 하고 있다. 항공 부문은 9·11 테러 이전부터 비교적 거의 완벽하게 물류보안 시스템을 구축, 시행하고 있다. 그 동안 세계적으로 무수히 많은 항공기 납치 사건(hijacking)이 발생함에 따라 국제민간항공기구(ICAO) 등에서 여러 가지 대응방안을 도입한 덕분이다.

이에 따라 현재 건설교통부에서 시행하고 있는 물류보안제도도 거의 대부분 항공부문에 치중되어 있다. 예컨대 2002년부터 전면 개정해 시행하고 있는 항공안전 및 보안에 관한 법률⁵⁰⁾과 이른바 ‘상용화주제도(known shipper)’가 대표적이다. 또한 항공보안에 관해서는 <표 3-2>에서 보는 바와 같이 고시나 지침 형태로 여러 가지 법적 장치가 마련되어 있다.

49) 사정이 이렇어도 불구하고, 실제 부산항 감만 터미널의 컨테이너 화물 검색시스템 설치 작업은 다소 지연되고 있음. 미국이 제공하는 컨테이너 화물 검색기(SAIC P7500)의 안전성 검토가 당초 예상보다 늦어지고 있기 때문임. 항만 관계자에 따르면, 설치 공사가 마무리되는 2007년 안에는 100% 검색 시범 사업에 착수할 수 있을 것으로 예상되고 있음.

50) 이 법률은 1974년에 제정된 항공기운항안전법에 근거를 두고 있으며, 2002년에 현재의 명칭과 같이 전면 개정됐음.

기존 법률을 항공안전 및 보안에 관한 법률로 전면 개정한 이유를 개정 사유를 통해 살펴보면 다음과 같다. “민간 항공기(民間航空機)의 운항안전(運航安全)을 증진시키기 위하여 보안검색(保安檢索), 항공안전 및 보안에 관한 기본계획의 수립, 항공안전보안지시·조사 및 점검 등에 대한 법적 근거를 마련함으로써 법 적용의 실효성을 확보하고, 민간항공의 안전성(安全性)·정시성(定時性) 및 효율성(效率性)을 유지하여 항공기와 탑승객(搭乘客)의 안전한 운항이 가능하도록 하는 등 현행제도의 운영과정에서 나타난 일부 미비점을 개선·보완하기 위한 것”이다.⁵¹⁾

<표 3-2>

우리나라 항공보안 관련 법규

법 명	법령 제정 기관
항공안전 및 보안에 관한 법률	건설교통부
보안검색 교육기관 지정 및 운영기준	항공안전본부
항공안전보안장비 종류, 성능 및 운영기준	항공안전본부
항공화물보안기준	항공안전본부
항공보안감독관 업무규정	항공안전본부
국가민간항공보안교육훈련지침	항공안전본부
공항건설 및 유지보수에 관한 보안지침	항공안전본부
국가항공보안수준관리 지침	항공안전본부
국가보안목표관리지침	국가정보원

자료 : 한국해양수산개발원

이 같은 목적을 달성하기 위해 우리나라는 i) 항공안전본부를 설치·운영하는 한편, ii) 항공안전 및 보안에 관한 기본 계획을 수립, 시행하고 있다. 또한 iii) 공항 운영자에 대해 공항시설 및 항행안전시설에 대한 안전 및 보안조치를 하도록 하는 한편, iv) 항공운송 사업자에 대해서는 항공기가 공항에 도착한 때에는 통과 또는 환승 승객이 휴대물품을 가지고 내리도록 하고, 보안검색을 완료한 후 탑승하도록 하는 등 여러 가지 보안 의무를 부여하고 있다.

또한 건설교통부는 항공보안을 강화하고, 물류 흐름을 촉진하는 방안의 하나로 상용화주제도를 2005년부터 도입하였다. 이 제도를 시행하기 위해 건설교통부는

51) 법제처(moleg.go.kr), 종합법령정보 검색 자료(2007년 6월 19일) 인용.

2004년 8월에 항공화물보안기준을 제정하였다.⁵²⁾

이 제도는 정기적으로 항공편(화물기)을 이용하는 화주나 대리점을 상용화주로 지정하고, 상용화주가 사전에 보안을 통제할 화물에 대해서는 항공사의 보안검색을 간소화하는 것을 말한다.⁵³⁾ 미국과 유럽연합 등에서는 이미 1990년대 중반부터 이와 유사한 제도를 실시하고 있다. 이들 국가들은 이 제도를 통해 화물 운송 지연을 줄여 운송의 적시성(適時性)을 높이는 한편, 물류보안을 강화하는 등 여러 가지 효과를 거두고 있다.

그러나 우리나라의 경우 이 제도 도입 이후 상용화주로 지정된 사례가 많지 않아 그 의미가 퇴색되고 있다.⁵⁴⁾ 또한 이를 이용하도록 되어 있는 화주와 항공사의 호응도도 매우 낮은 것으로 알려졌다. 이에 따라 정부는 최근 상용화주를 지정·감독하는 주체를 현재의 항공사에서 정부 또는 정부가 위탁한 제3의 기관으로 변경한다는 개선안을 발표한 바 있다. 현재처럼 항공사가 상용화주를 자체적으로 지정·관리해야 할 경우 항공사의 입장에서는 화물보안 확보를 위해 이중의 의무를 지게 되고, 자의적인 화주지정으로 인한 논란이 발생할 가능성도 배제할 수 없기 때문이다.

한편, 이 제도가 본래 취지대로 자리매김을 하기 위해서는 다음과 같은 사항을 추가적으로 검토할 필요가 있다는 의견도 제시되고 있다. 먼저 화주의 적극적인 참여를 유도하기 위해서는 이 제도가 화물의 흐름을 촉진시킴으로써 화주들에게 궁극적으로 득이 된다는 사실을 인식시켜야 한다. 상용화주 등록을 위해 화물보안 프로그램을 마련하는 등 추가비용을 부담해야 하는 화주들의 경우 비용편익에 대한 확신 없이는 신설 제도의 활용에 소극적일 수밖에 없기 때문이다.

이와 함께 국제 환경변화에 대비하는 수단으로 상용화주제도가 이용될 수 있다는 점도 알릴 필요가 있다. 미국이 상용화주의 등록을 의무화하고, 경제협력개발기구(OECD)에서도 이를 기반으로 하는 물류보안제도를 도입하는 등 화주의 운송

52) 건설교통부 항공안전본부 고시 제25호.

53) 상용화주라 함은 항공운송사업자와 항공화물 보안통제에 관한 서면협약을 체결하여 지정된 자로서, 공항 이외의 지역에서 항공화물을 최초로 포장하여 보관 및 운송을 하는 자(이하 “지정화주”라 한다) 또는 화주가 운송을 의뢰한 항공화물에 대한 보안통제를 실시하는 자(이하 “지정대리점”이라 한다)를 말함(항공화물 보안기준 제3조).

54) 이 제도를 도입한 지 2년이 지난 2006년 12월에야 비로소 우리나라 삼성전자 로지텍이 상용화주로 처음 지정됐음. 건설교통부는 이 같은 상용화주제가 본래 도입 의도와 다르게 활용도 낮은 것으로 나타남에 따라 제도를 활성화하는 방안을 모색하고 있음(한국해양수산개발원 외, 2007 국제물류보안 동향 및 대응전략 세미나, 2007. 10. 23).

보안 의무가 점차 강화되고 있는 점을 관심 있게 지켜볼 필요가 있다. 앞에서 언급한 물류보안 인증제도 역시 정도에서는 차이가 있으나 사실상 상용화주제도와 궤를 같이 한다.

3) 다른 부처

두 부처 이외에 관세청과 국가정보원도 물류보안과 직·간접적으로 연결되어 있다. 관세청은 미국과 체결한 컨테이너 보안협정(CSI)의 시행주체라는 점에서, 국가정보원은 국가 안보보장을 담보하는 부처의 하나라는 점에서 각각 물류보안 업무를 수행하고 있다.

첫째, 관세청은 언급한 바와 같이 2003년에 미국 세관·국경보호국(CBP)과 컨테이너 보안 협정(CSI)을 체결하였다. 이에 따라 부산항에서 미국행 컨테이너 화물에 대한 사전 검색작업을 실시하고 있다. 미국 또한 CSI 제도를 원활하게 수행하고, 우리나라에서 실시하는 검색활동을 지원하기 위해 8명 정도의 검사관을 파견·주재시키고 있다.

이와 함께 관세청은 외국에서 우리나라로 수입되는 컨테이너 화물에 대한 밀수 및 보안 검색활동도 강화하고 있다. 관세청은 이 사업을 추진하기 위해 2006년 말 현재 모두 10대의 컨테이너 화물 검색기를 도입·운영하고 있다. 관세청은 앞으로도 연차 계획에 따라 장비를 추가 설치할 계획이다. 관세청은 또한 최근 WCO 등을 중심으로 컨테이너 화물에 대한 안전성을 강화함에 따라 국제간 이동하는 컨테이너를 감시·추적하는 모니터링 사업을 추진하고 있다. 2007년 7월 관세청이 벨기에 당국과 양해각서(MOU)를 체결한 것도 이 같은 사업을 진행하기 위한 준비작업이라고 할 수 있다.

둘째, 국가정보원은 우리나라 물류보안을 촉진하고, 보다 효율적으로 추진하는 것을 지원하기 위해 2007년에 ‘물류보안체제 구축 민·관 협의회’를 구성해 운영하고 있다. 이 협의회에는 국가정보원을 포함, 해양수산부 건설교통부, 외교통상부, 관세청 등 물류보안과 관련되어 있는 정부 부처뿐만 아니라 한국무역협회, 한국선주협회, 삼성물산 등 이해관계 업체 다수가 참여하고 있다. 특히 이 협의체는 정부 각 부처에서 시행하고 있는 물류보안 현안을 검토하는 한편, 민간기업이 물류보안을 추진하는 과정에서 나타날 수 있는 문제점을 해결하는데 주력하고 있다.

<표 3-3>

우리나라 항만의 컨테이너 화물 검색기 설치 현황

입찰 년도	형식	투과력 (철판 mm)	제조사	낙찰가 (백만원)	설치항
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
2006	조립이동식	380			인천항

자료 : 관세청

2. 우리나라 물류보안제도의 문제점

우리나라 물류보안 문제점은 어떤 의미에서 보면 외생변수라 할 수 있다. 2001년 9·11 테러 이후 국제적으로 물류보안이 강화되고 있는 글로벌 환경 변화로 야기된 것이 대부분이기 때문이다. 그러나 연구진이 조사한 바에 따르면, 물류보안이 국제적으로 강화되기 시작한 지 5년이 지났음에도 우리나라의 경우 아직 물류보안에 대한 이해가 여전히 낮은 것으로 나타났다. 정부와 민간 부문의 인식도 크게 부족한 것이 현실이다.

1) 제도적인 문제점과 향후 과제

(1) 물류보안제도가 정립되어 있지 않음

우리나라가 안고 있는 가장 문제점은 화물 공급 사슬 전반을 통합적으로 관리하는 물류보안제도가 구축되어 있지 않다는 점이다. 미국의 C-TAT의 경우 제품 생산에서 판매에 이르는 전 구간의 완벽한 보안 확보를 요구하고 있으며, 유럽연

합이나 싱가포르 등도 이 같은 추세에 따르고 있다. 또한 APEC이 최근 물류보안에 관한 가이드라인을 발표하고, 회원국의 자발적인 이행을 촉구하고 나선 것에 주목할 필요가 있다.

특히 APEC은 기존에 국제사회에서 논의하던 방향에서 더 나아가 테러 이후 교역을 신속하게 재개할 수 있는 방안까지 물류보안제도에 포함하였다. 지금까지 테러 예방과 차단에 주력하던 물류보안제도가 테러 이후의 대책까지 그 범위가 더욱 확대된 것으로 해석된다. 앞으로 우리나라가 보다 완벽한 물류보안제도를 도입할 때는 이 부문까지 관심을 기울여야 한다는 것을 의미한다.

(2) 물류보안업무 수요가 파악되어 있지 않음

더 큰 문제는 국제적으로 물류보안제도가 강화되고 있음에도 일부 부처와 기업을 제외하고, 이 같은 움직임을 정확하게 파악하지 못하고 있다는 점이다. 물류보안을 담당하는 부처에서 정확하게 무슨 일을 해야 하는지 업무 분장도 사실은 거의 없다고 해도 과언이 아니다. 게다가 각 부처에 분산되어 있는 물류보안 업무를 통합·조정할 수 있는 기능이 없을 뿐만 아니라 이를 관장하는 기본계획도 마련되어 있지 않은 실정이다.

이 같은 문제점이 잉태된 것은 물류보안제도가 태동한 지 일천한 데도 원인이 있으나 기본적으로는 물류보안제도에 대해서 그 동안 우리나라가 너무 수동적으로 대처해온 데도 이유가 있는 것으로 판단된다. 따라서 앞으로는 각 정부 부처에서 물류보안제도를 확립하기 위해 무엇을 해야 하는지 정확하게 업무 수요를 파악하는 것이 중요하고, 통합적인 차원에서 물류보안을 추진할 수 있는 대안을 마련할 필요가 있다.

(3) 물류보안 기준이 마련되지 않은 상태

이 같은 문제뿐만 아니다. 우리나라의 물류보안과 관련해 가장 현실적으로 직면한 문제점은 “물류보안을 어떻게 해야 하는지 마땅한 기준이 없다”는 점이다. 즉, 물류부문에 종사하는 기업이 어떤 기준에 입각해 보안을 확보해야 하고, 기업이 자체적으로 도입·시행하고 있는 물류보안 시스템이 옳은 것인지 판단할 근거가 없다는 것이 문제점으로 지적되고 있다.

우리 원이 이 연구를 진행하던 과정에서 개최한 자문회의에 따르면, 거의 대부분의 전문가들이 지적한 문제점은 다음과 같다.

첫째, 물류보안제도가 국제적으로 도입되기 시작한 지 5년이 경과했음에도 아직까지 우리나라에서는 이를 이행하는 주체가 명확하게 가려지지 않았다는 점이다. 따라서 앞으로 우리나라가 물류보안제도를 정립할 때는 적용 대상 기업이나 범위를 명확히 할 필요가 있다.

둘째, 물류보안과 관련해 기업이나 정부가 무엇을 할지 분명히 해야 한다는 지적도 나왔다. 다시 말하면, 물류보안과 관련된 정부의 기능과 역할을 설정하는 한편, 참여하는 기업이 물류보안제도를 이행하기 위해 ‘해야 할 일에 대한 기준’을 제시하는 것이 화급하다는 주문이다. 예컨대, 원자재 공급업체나 제조기업, 창고업체, 그리고 화물 운송업체나 컨테이너 터미널 운영회사 등이 물류보안을 확보하고, 이행하는데 필요한 법적 기준을 마련하는 것이 시급하다.

(4) 국가간 물류보안 협력사업도 미흡

또한 물류보안을 강화할 수 있는 민·관 협력 프로그램이 부족하고, 전문가 양성이나 국제 협력 등에 거의 관심을 기울이지 못하고 있는 것이 우리나라 현실이다. 싱가포르와 홍콩, 일본, 중국 등이 자국의 보안기준을 글로벌 기준에 맞추는 한편, 이 같은 흐름을 적극 활용해 환적 화물 유치에 물론 궁극적으로 국제 경쟁력을 높이는 지렛대로 활용하는 전략을 추진하고 있는 것과는 대비된다.

특히 우리나라 주변에 있는 일본과 중국의 경우 물류보안에 관한 한 우리나라보다 발 빠른 대응을 하고 있어 주목된다. 일본은 미국과 물류보안협력을 강화하기 위해 지난 4월 미국과 물류보안 상호 인증제를 도입하기로 하는 등 적극 대응하고 있는 것으로 나타났다.

즉, 미국과 일본은 물류비용을 줄이고, 통관절차를 간소화하기 위해 서로 시행하고 있는 수출 컨테이너 화물의 보안검색제도를 상호 인증하는 방안을 검토하기로 합의하였다. 일본은 9·11 테러 이후 미국과 컨테이너 보안협정을 맺고, 도쿄와 요코하마, 나고야, 고베에서 미국행 컨테이너 화물에 대한 사전 검색작업을 해 왔는데, 상호인증제도가 도입되면, 화물 통관시간이 2일 정도 줄어들 것으로 보여 제조업체 및 물류기업의 경쟁력을 향상시키는데 큰 도움을 줄 것이라는 전망이 나오고 있다.⁵⁵⁾

중국 또한 예외는 아니다. 2006년 남중국 선전항만이 중국 세관과 공동으로 유럽연합(EU)과 컨테이너 화물 추적 시범사업에 착수한 데 이어 상하이 국제 항무집

55) JOC, 2007년 4월 10일자.

단(SIPG)도 유사한 사업을 2007년 6월부터 미국 조지아 주 항만 당국과 공동으로 추진한다고 발표했다. 특히 중국이 미국과의 컨테이너 화물 추적 시범사업을 추진하는 과정에서 사비 네트워크(Savi Networks)와 함께 개발한 컨테이너 봉인장치(E-seal)를 실험하는 한편, 유럽지역까지 이를 확대할 계획이다.⁵⁶⁾ 우리나라가 앞으로 외국과 물류보안협력을 강화해야 하는 이유가 여기에 있다.

(5) 기존 물류보안제도의 허점도 많음

또한 우리나라는 내륙 운송부문의 경우 물류보안을 담보할 수 있는 법적 기반이 없어 도로 및 철도의 경우 테러 등 위협사태에 그대로 노출되어 있는 실정이다. 예컨대, 제품의 원료를 조달하는 단계에서 생산하고, 컨테이너에 적입한 다음 이동하는 과정에서 보안통제가 전혀 이루어지지 않고 있다. 물론 트럭이나 철도 등으로 운송되는 컨테이너에 대한 추적도 아직은 먼 나라의 일이다.

또한 항만에서는 컨테이너를 적재한 트럭이 항만 게이트를 통과할 때 운전기사에 대한 통제와 신분확인이 이루어지지 않고 있는 실정이다. 항만의 경우 2004년 7월부터 ISPS 코드 시행으로 보안상태가 많이 개선됐으나 형식적인 대처가 많다는 지적도 제기되고 있다. 예컨대 항만 감시 카메라의 경우 관세청과 항만 경비보안업체가 별도로 운영하고 있어 예산낭비가 아니냐는 지적이 있다. 일부 터미널의 경우 물류보안에서 가장 기본적인 출입자 통제조차 제대로 이루어지지 않고 있다.

또한 항공부문도 외국 항공사의 보안 검색 능력문제, 상용화주제도 도입문제, 보안 경비요원의 능력과 높은 이직률, 고도화되는 테러에 대한 대체 능력이 부족하다는 등 여러 가지 문제점이 제기되고 있는 것이 오늘날 우리나라 물류보안의 현실이다.

2) 기술적인 문제점과 향후 과제

(1) 물류보안산업의 활용·투자 미흡

물류보안이 글로벌 메가 트렌드로 정착하면서 이와 관련된 시장도 급성장하고 있다. 물류보안시장이 향후 새로운 성장산업으로 떠오르고 있기 때문이다. 전문가들은 앞으로 기업이나 정부를 막론하고, 물류 전구간의 완벽한 보안 시스템을 구축해야 하므로 앞으로 시장 규모가 상당히 커질 것으로 전망하고 있다.

컨테이너 화물 검색기, 전자 태그를 기반으로 하는 컨테이너 봉인장치, 항만 출

56) CI, 2007년 6월 18일자.

입보안 시스템, 스마트 컨테이너 등 하드웨어뿐만 아니라 기업에 대한 물류보안 인증 및 물류보안 컨설팅, 물류보안 전문가 육성 및 교육에 이르기까지 물류보안 시장이 크게 확대될 수 있다.

글로벌 기업들은 현재 이 같은 물류보안 시장을 선점하고, 확대하기 위해 적극 나서고 있다. 컨테이너 보안장치를 둘러싸고, 록히드 마틴 그룹(사비 네트워크)과 미국의 제너럴 일렉트릭(GE) 등 7개 글로벌 기업 컨소시엄이 참여하게 대립하고 있는 것이 대표적인 사례라 할 수 있다. 이뿐만 아니다. 컨테이너 화물 검색기 개발 및 상용화와 관련해서는 미국의 SAIC사와 스미스 디텍션사, 그리고 중국 칭화 대학의 벤처 기업에서 글로벌 전문기업으로 성장한 누크테크(Nuctech)사 등이 시장 점유율을 높이기 위해 경쟁하고 있다.

따라서 우리나라가 앞으로 물류보안 장비 및 기술개발과 투자, 외국과의 물류보안 협력을 소홀히 할 경우 향후 국제 표준 경쟁에서 낙오되는 것은 물론 엄청난 기술 도입료(이른바 특허 사용료)를 부담해야 하는 부담도 떠안게 될 가능성도 있다.⁵⁷⁾

(2) 항만 물류보안시스템 구축도 소홀

한편, 현재 국제적으로 강화되고 있는 물류보안제도를 최종적으로 이행하는 것은 항만이라 해도 과언이 아니다. 이 곳에서 수·출입되는 모든 화물에 대한 검사가 이루어지기 때문이다. 즉, 항만은 수출하는 화물에 대해서는 최종 선적지가 되고, 수입하는 화물에 대해서는 최초 도착지가 되기 때문에 다른 지역에 비해 물류보안이 특히 강조되고 있다. IMO에서 ISPS 코드를 제정해 항만의 보안을 강화하고, 미국이 9·11 테러가 일어난 직후 세계 20대 대형항만을 대상으로 컨테이너 보안협정(CSI)을 시행한 이유도 여기에 있다.

따라서 항만에 보다 완벽한 물류보안 시스템을 구축하는 것이 시급하다. i) 화물에 대한 통제, ii) 인력에 대한 관리, 그리고 iii) 항만 시설에 대한 치밀한 보안 시스템을 구축할 필요가 있다. 이와 관련해 우리나라는 ISPS 코드를 시행하는 과정에서 항만시설에 대한 보안 시스템은 어느 정도 확보된 것으로 평가되고 있다. 앞으로는 출입하는 인력과 화물에 대한 관리를 더욱 강화하는 노력이 필요하다.

특히 우리나라에는 수출 컨테이너 화물을 전용으로 검색할 수 있는 시스템이

57) 우리나라 부산항과 경쟁관계에 있는 중국 상하이 항만의 경우 항만 운영 효율화와 물류보안 강화라는 두 마리 토끼를 잡기 위해 전자 태그를 기반으로 하는 컨테이너 추적 및 봉인 시스템을 개발하고, 2007년 6월부터 미국 조지아 주 항만당국과 시범 사업에 착수했음. 이에 앞서 남중국의 선전 항만도 상하이 항만과 유사한 사업을 유럽연합(EU)과 지난해부터 시작한 바 있음.

구축되어 있지 않은 것이 큰 문제점의 하나로 지적되고 있다. 현재 설치되어 있는 화물 검색기는 주로 수입 컨테이너를 검색하는데 활용되고 있기 때문이다. 또한 우리나라 시스템은 단순히 컨테이너 내장 화물을 영상 검색하는데 한정되어 있다. 다른 나라에서 사용되고 있는 최첨단 화물 검색기가 OCR, 영상 검색 및 방사능 탐지 등 3가지 기능 일체형(ICIS)이라는 점에서 우리나라와 차이가 있다는 지적이다.

그런데 문제는 이 같은 시스템을 구축하기 위해서는 국산 장비를 사용하거나 외국에서 장비를 구입해야 하는데, 컨테이너 화물 검색기 개발에 관한 우리나라의 기술 인프라도 열악하다는 점이 문제다. 일부 업체에서 화물 검색기를 개발하였으나 사용실적이 없어 입찰에서 탈락한 것으로 알려졌다. 이에 따라 선진국 수준에 맞추기 위해서는 ‘시스템 일체형 컨테이너 화물 검색기’ 개발이 절실한 실정이다. 이 부문에 대한 정부의 기술개발(R&D) 투자가 절실하다.

(3) 컨테이너 화물 추적 서비스 여건 미흡

국제적인 물류보안의 핵심은 오직 하나다. 국제적으로 이동하는 컨테이너가 완전무결하다는 점을 서로 보장하는 것이다. 지금까지 언급한 거의 모든 물류보안제도가 궁극적으로 추구하는 목표는 단 한 가지, 컨테이너에 무엇이 들어 있는지 사전에 확인하고, 이른바 대량살상무기(WMD)가 다른 나라로 밀반입되는 것을 차단하는데 있다.

이 같은 이상을 충족시키기 위해 고안해 낸 것이 CSI와 24시간 규칙이다. 미국의 C-T PAT와 WCO의 SAFE Framework도 마찬가지다. 문제는 현재 이 같은 제도를 유기적으로 연결하는 하드웨어가 부족하다는 점이다.

즉, 기업에서 생산한 제품이 컨테이너에 적입된 두 트럭 등 육상 운송수단에 실려, 항만을 거쳐 외국의 최종소비자에 이르는 전 물류구간을 추적·통제할 수 있는, IT와 결합된 물류보안 솔루션이 아직 우리나라에서는 개발되지 않은 실정이다. 앞으로 i) 컨테이너 화물정보를 관리하고, ii) 전자 태그를 활용한 컨테이너 잠금 및 봉인 장치 개발과 함께, iii) 이 같은 장치를 부착한 컨테이너가 운송되는 전 과정을 실시간으로 모니터링 하는 것은 물론, iv) 운송 도중에 부정개폐 등 문제가 발생한 경우 이를 해결하는 방안이 포함된 ‘통합 물류보안 시스템’을 구축할 필요가 있다. 또한 이 시스템을 구축, 상용화하는 경우 엄청난 부가가치를 창출할 수 있다.

제4장 국가 물류보안체제 확보 방안⁵⁸⁾

제4장에서는 지금까지 언급한 사항을 토대로 앞으로 우리나라가 물류보안체제를 확보하기 위한 전략을 중점적으로 언급한다. 현재 국제적으로 강화되고 있는 물류보안에 대비하기 위해서는 계획과 제도, 인프라, 그리고 국제협력 측면에서 많은 개선이 필요하다. 이러한 관점에서 제4장에서는 이 같은 추세를 반영하여 1) 국가 물류보안계획 수립·시행을 통한 우리나라 물류보안체제 개편 방안과 2) 물류보안 위기관리 및 복구대책을 중심으로 정책방안을 제시한다.

1. 국가 물류보안체제의 개편

우리나라의 물류보안체제를 개편하는 방안은 두 가지 차원에서 검토가 가능하다. 하나는 새로운 법률 등을 제정하여 기존의 제도를 보완하는 방법이 그것이다. 또 하나는 기존의 제도를 그대로 둔 채 일정한 형식의 국가 물류보안계획을 수립하여 시행하는 방안이다.

전자의 경우 기존 법률에 반영되지 않은 사항이나 흠결 부문을 새로운 법률에 담아 시행하는 것이므로 보다 완벽하게 우리나라 물류보안체제를 개편하는 방안이 될 수 있다. 그러나 이 같은 방법에 따를 경우 입법과정이 번거롭다는 단점이 있을 뿐만 아니라 물류보안 관계 부처 간의 협의 등에서 여러 가지 난관에 봉착할 가능성도 있다는 흠도 있다. 후자는 기존의 관련 법률에 근거해 법정계획 형식으로 새로운 국가 계획을 수립·시행하는 것이므로 절차와 방식에서 다소 용이하다는 이점이 있다. 또한 관계 부처 사이의 협의를 거쳐 특정 부처에서 계획의 수립과 집행을 주도할 수 있어 제도 개편에 따른 실효가 크다는 장점이 있다. 이에 따라 이 연구 보고서에서는 우리나라 물류보안을 확립하는 대안의 하나로 가칭 ‘국가 물류보안 계획’을 수립하는 것을 제시하고, 계획에 반영될 사항을 아래와 같이 검토하였다.

58) 한편 해양수산부에서는 국가 물류보안체제를 실질적으로 구축하기 위해 「항만·물류보안체제 구축 실용화 방안 연구사업」 용역을 2007년(8월~12월)에 실시하였다. 여기에는 물류보안 업무수요 조사 및 정책우선순위 결정, 물류보안제도 도입 및 지침 수립, 물류보안 인증제도 및 운영방안, 항만 인적보안 시스템 구축방안설계, 컨테이너 보안장치 도입방안, 항만물류 정보센터 구축방안 등이 포함되어 있다.

1) 국가 물류보안계획 수립·시행

국가 물류보안계획에는 1) 우리나라 물류보안에 관한 기본 방침과 2) 중장기 정책방향을 정하고, 3) 각 부처별 국가 물류보안체제 구축에 관한 사항을 정한다. 따라서 제1절에서는 국가 물류보안계획에 포함되어야 하는 사항을 집중적으로 검토하였다.

다만, 문제는 이 같은 계획을 수립·시행하는 경우 법률에 근거해 시행하는 것이 바람직하므로 관련법령을 검토하는 것이 필요하다. 현재 국가물류보안계획을 수립하는데 근거조항으로 인용할 수 있는 법률은 크게 2가지가 있다. 물류정책기본법과 국제 항해선박 및 항만시설보안에 관한 법률로 모두 올해 국회에서 제정되었다. 전자의 경우 건설교통부장관과 해양수산부장관은 국가 물류정책의 대강을 정하고, 10년마다 국가 물류기본계획을 수립·시행하도록 정하고 있다. 따라서 이 계획의 내용에 물류보안확보에 관한 사항을 반영하는 방안이 있다. 또 다른 대안으로는 후자의 법률 내용을 인용하는 것인데, 이 법률에는 해양수산부장관으로 하여금 국가항만보안계획을 수립·시행하도록 규정하고 있다. 따라서 이 계획 속에 물류보안 확보에 관한 사항을 포함하는 방안이 있다.

문제는 이 같은 방안에 따를 경우 이 곳에서 제시하는 ‘국가물류보안계획’이 다른 계획에 묻혀 국가 계획으로서의 독자성을 상실할 우려가 있다는 점이다. 따라서 이 같은 문제점을 해결하기 위해서는 특정 법령에 근거를 둘 것이 아니라, 별도의 계획을 수립하여 국무총리가 위원장이 되고, 경제부처 장관들로 구성된, 경제정책 조정회의의 의결을 거쳐 시행하는 방안이 있다.

(1) 물류보안계획 기본 방침

국가 물류보안계획을 수립하는 정책 목표, 즉 기본 방침은 현재 국제적으로 강화되고 있는 물류보안제도를 국내에서 시행할 수 있는 기반을 마련하는 것과 이를 발판으로 국가 물류 경쟁력을 확보하는데 초점을 맞추는 것이 바람직하다. 글로벌 물류보안제도는 테러 예방이라는 긍정적인 측면에도 불구하고, 제도를 시행하는 과정에서 정부 및 기업 부문에 적지 않은 부담을 줄 우려가 있다. 따라서 이 같은 부담을 최소화하면서 외생적인 변수에 의해 도입되는 제도를 활용하는 전략을 마련하는 것이 중요하다. 이러한 점을 고려하여 국가 물류보안계획의 기본 방침으로는 ‘글로벌 물류보안제도를 활용한 국가 물류경쟁력 강화’로 정책 목표를 설정하

고, 다음과 같이 시행 기본 방침을 고려할 필요가 있다.

첫째, 글로벌 물류보안 강화 추세에 적극 대응하는 물류보안체제를 구축한다. 둘째, 동북아 인근 항만에 앞서 신속하게 물류보안체제를 구축함으로써 항만 경쟁력을 확보하고, 차별화된 부가가치를 창출한다. 셋째, 물류보안에 관한 업무를 원활하게 추진하기 위해 해양수산부 등 물류보안 관련부처가 참여하는 물류보안정책 협의체를 구성하여 운영한다.⁵⁹⁾ 넷째, 물류보안제도를 조기에 정착하기 위해 민간부문의 자발적인 참여를 유도하는 방안을 마련한다. 다섯째, 물류보안산업을 육성하고, 비즈니스 모델을 개발하는 등 정책 지원을 강화한다. 여섯째, 물류보안의 국제적 확산에 필요한 대외협력을 강화한다.

(2) 물류보안계획 중장기 정책 방향

국가 물류보안계획에 반영될 중장기 정책 방향은 아래의 그림에서 제시된 바와 같이 3가지 축을 기본 구조로 추진하면 될 것으로 판단된다.

<그림 4-1>

중장기 물류보안 정책 추진 로드맵



59) 국가정보원이 2007년 3월부터 국가물류보안체제 구축 민관협의체를 구성·운영하고 있으므로 이 기구를 확대 개편하는 방안도 가능할 것으로 판단됨.

<표 4-1>

각 부처별 물류보안 추진 업무

부처별	추진사업		관련부처
해양수산부	기존	• ISPS 코드 이행	단독
	향후	• 국제선박 및 항만시설 법률시 이행 국가 항만보안계획 수립·이행 항만 보안료 부과·징수	단독
		• 전자 태그 활용사업 화물 컨테이너 전자봉인 부착 화물정보 및 물류보안 정보시스템 구축 컨테이너 화물추적 시범사업	산자부 건교부 관세청
		• 컨테이너 화물 검색기 설치·운영 - 국가 항만보안계획에 포함	관세청
		• 물류보안 인증 사업 항만·터미널 운영업체·선사 등 물류기업 사업장 경영 보안 인증	건교부 관세청 산자부
		• 항만물류보안 솔루션 개발·상용화 - 항만·인적·물적 보안시스템 구축	단독
		• 물류보안교육훈련 프로 개발 운영 교육훈련제도·교육기관 기능 강화 교육·훈련 전문인력 양성 교육·훈련 자료 개발 보급	단독
건교부	기존	• 상용화 주체 시행	단독
	향후	• 내륙 부문 보안제도 도입	단독
		• 컨테이너 화물 추적사업	단독
		• 종합 물류기업 보안인증	해양부·관세청
산자부	향후	• 물류기업 경영보안 인증제 도입 시행	해양수산부·관세청
	향후	• 물류보안 표준의 제정·시행 컨테이너화물 검색기 컨테이너 전자봉인 컨테이너 화물용 전자 태그	해양수산부 관세청

자료 : 한국해양수산개발원

즉, 국가 물류보안 계획의 수립·시행을 통해 국가 물류보안체제를 확립한 뒤 물류보안 서비스를 확대하고, 장기적으로는 물류보안 서비스를 고도화함으로써 항만의 부가가치를 높이는 한편, 물류경쟁력 제고라는 정책 기본 목표를 달성할 수 있도록 연결고리를 마련하면 될 것이다. 특히 국가 물류보안계획의 세부이행방

안에 각 물류 구간마다 시행되어야 하는 사항도 정함으로써 실제 물류활동에 종사하는 기업이나 정부 부처에서 향후 어떠한 사항을 추진하고, 이행해야 하는지 ‘추진 일정표(로드맵)’를 마련한다.

(3) 각 부처별 물류보안 시행 사항

초기와 달리 현재 국제적으로 시행되고 있는 물류보안제도는 해양수산부, 관세청 등 여러 정부 부처의 업무와 관련되어 있는 것이 특징이다. 따라서 한 정부 부처에서 물류보안제도를 독자적으로 추진하기는 현실적으로 가능하지도 않을 뿐더러 부담도 큰 것이 사실이다.

이 같은 점을 고려할 때 물류보안제도는 정부조직법에 정해진 바와 같이 소관 부처에 관련 업무를 추진하도록 하는 것이 바람직하다. 다만, 업무 추진에 따른 일관성을 확보하고, 시너지 효과를 제고하기 위해서는 해양수산부 등 특정 부서에서 국가물류보안정책을 통괄하는 것이 바람직한 것으로 판단된다. 국가물류보안 계획에 반영될 각 소관 부처별 향후 추진업무를 정리하면 다음과 같다.

2) 물류보안 협력사업 추진

(1) 필요성

21세기 글로벌 시대에서 국가 간 협력은 글로벌 이슈 해결의 시발점이 되고 있다. 특히 글로벌 이슈가 국가안보 및 글로벌 무역과 관련된 경우는 더욱 그러하다. 물류보안도 마찬가지다. 물류보안은 화물과 함께 실려 오는 국가안보 위협, 즉 테러와 이에 상응하는 사건에 대응해 국가 안보를 확보하는 한편, 글로벌 무역의 원활화를 확보하기 위해 필요한 것이다. 그리고 이러한 물류보안 확보를 위해서는 국가 간 협력이 반드시 전제되어야 한다.

그렇다면 물류보안에서의 협력은 어떠한 방향으로 전개되어야 하는가? 우선 국내 협력이 우선되어야 한다. 국내 협력이란 크게 관련 정부부처간의 협력과 정부 부처와 관련 기업간의 협력을 말한다. 다시 말하면 물류보안은 물류 공급망 보안과 동일한 개념이어서 물류 공급에 참여하는 모든 주체, 즉 정부 부처의 경우, 관세청, 해양수산부, 산업자원부, 건설교통부 및 국정원, 관련 기업의 경우, 제조업자, 수출입업자, 해운 및 내륙운송업자 등의 협력이 바탕이 되어야 한다. 이러한 국내협력 틀이 마련된 후 국가 간 협력은 탄력을 받게 된다.

국가 간 협력은 국제사회라는 공공의 장소에서 국가 간의 양자협력과 국제기구를 중심으로 한 다자협력으로 나눌 수 있다. 또한 이러한 국제협력은 법적 구속력 있는 협력(예 양자 및 다자협정)과 구속력은 없지만 합의를 통해 스스로를 구속하는 협력(예 framework나 declaration 등)으로 대변된다.

그럼 구체적으로 물류보안과 관련된 협력이 어떻게 이뤄지고 있는지에 대해서 한 번 살펴보기로 한다. 우선 국내협력 차원에서는 비공식기구로서 ‘물류보안 민관협의회’가 운영되고 있으나 물류보안을 전담하거나 협력을 모색하는 기구는 아직 없다. 다만 관련 정부부처인 해수부, 관세청, 건교부 및 국정원 등에서 각기 이에 대한 대응책 마련을 위한 논의가 진행 중이다. 이는 국제사회의 움직임에 비해 뒤쳐져 있지 않아 보이지만, 이러한 움직임이 대부분 사회적 합의나 공감대를 형성하지 못하고 있는 상황에서 이뤄지고 있어 그 추진력은 약하다. 또한 물류모드별로 협력체계가 구축되어야 완벽한 물류보안을 달성할 수 있음에도 불구하고 그러한 움직임은 눈에 띄지 않고 있다.

그렇다면 국가 간 협력을 위한 현황은 어떠한가? 우선 적극적으로 물류보안에 대한 국가 간 협력에 나서고 있는 정부기관은 관세청이다. 관세청은 현재 WCO의 Framework에 따른 대응책으로 관세법 개정을 주도하고 있으며, 한-벨기에 관세청 간 시범사업을 추진하는 등 다른 부처보다 적극적인 모습을 보이고 있다. 또한 해양수산부도 항만보안을 중심으로 전개되는 물류보안의 국제적 흐름에 발맞추어 ISPS Code를 국내적으로 이행하기 위한 ‘선박 및 항만시설 보안에 관한 법률’을 제정하는 등 보다 능동적인 자세를 견지하고 있다. 하지만, 이러한 노력도 최근에 이뤄지고 있는 것들이며, 아직 다른 부처를 포함한 다차원적 국제협력 틀을 공고화하기 위한 방안마련이 시급한 것이 사실이다.

따라서 이제부터의 노력이 중요하다. 이를 위해서는 현재 국제사회와 각 국가에서 진행되고 있는 물류보안관련 국내 및 국제협력의 움직임을 살펴보는 작업이 필요하며, 이를 통해 향후 우리나라가 나아갈 방향을 제시하고자 한다. 결론을 먼저 말한다면 우리나라는 국내협력을 바탕으로 다차원적인 국제협력을 추구하는 ‘다층적 전략’을 추구해야 한다. 이러한 다층적 전략은 역으로 국내 정부부처 간 협력 및 타 국가와의 협력이 조화롭게 이뤄지는 그 정점에서 달성될 수 있는 것이다.

이하에서는 앞서 언급한 국내협력과 국제협력을 해외사례와 우리나라의 현황을 중심으로 살펴보고, 이를 통해 향후 우리나라가 ‘다층적 전략’ 마련을 위해 어떠한 노력을 기울여야 하는지에 대해서 살펴보기로 한다.

(2) 현황

가. 국내 정부부처 간 협력

① 국외사례

물류보안을 실시하고 있는 세계 주요 국가는 국내 정부부처 간 협력을 주요 축으로 삼고 있다. EU 및 캐나다, 싱가포르 등이 제시하고 있는 국내 정부부처 간 협력은 세관을 중심으로 이뤄지고 있는 반면, 미국은 국토안보부를 중심으로 보안 이슈를 조정하고 있다. 대표적으로 미국의 사례를 살펴보도록 한다.

미국의 대표적 물류보안 관련법인 항만보안법(Security and Accountability for Every Port Act of 2006 : SAFE Port Act)과 9.11 위원회 권고 이행을 위한 법률(Implementing Recommendation of the 9/11 Commission Act 2007 : 이하 9.11 이행법)은 이와 관련한 규정을 두고 있다. 우선 미국 SAFE Port Act Sec.205는 컨테이너 보안구상(Container Security Initiatives)과 관련해서 국토안보부 장관이 국내 무역대표부(USTR)와 국무부와의 협의를 거쳐 해외 정부기관과 CSI항만지정을 위한 협상을 하도록 규정하고 있다. Sec.233은 CSI지정항만에 대한 기술지원, 장비 및 교육지원과 관련해 국무부, 에너지부 및 적절한 연방정부와의 조정(Coordination)을 하도록 규정하고 있으며, 특히 해외항만과 미국영토에서의 행동 및 지원(Actions and Assistance for Foreign Ports and United States)법률 제46조 Sec. 70110을 개정하면서 해외의 항만보안이행 추진방안 마련에 관련된 연방기관과 협력하도록 규정하고 있다. 또한 Sec. 703은 트럭보안(Trucking Security)과 관련해 국토안보부 장관과 교통부 장관이 2004년 제정된 양해각서(Memorandum of Inspector General Of the Department of the Transportation)에 포함된 권고 이행규정마련을 위해 협력하도록 규정하고 있다.

또한 9.11 테러이행법 Sec.721은 인신매매 및 마약센터(Human Smuggling and Trafficking Center : HSTC) 설립에 필요한 인력구성문제를 국토안보부가 관련 정부기관과 협력하도록 규정하고 있다. 그리고 부수적으로 Sec.801에서 민간 프라이버시 감시위원회의 설립 및 운영과 Sec.1002에서의 인프라 보안과 관련한 위험평가부분에서 국토안보부를 중심으로 상무부 등 관련 기관과의 협력을 규정하고 있다.

이밖에 뉴질랜드는 2006년 초 관세청을 중심으로 테러, 불법이민, 유행성 질병 및 야생동물 밀수 등을 방지하기 위해 국가목표센터(National Targeting Center)를 설립하여 정부기관 간 협력을 도모하고 있다. 주목할 점은 이 센터를 통해 관세청

이 주도하여 대량살상무기의 국제거래를 감시하고 테러에 대항하기 위한 업무를 수행하기 위해 정부기관 간 정보교환 및 사후 신속한 해결을 도모한다는 것이다.

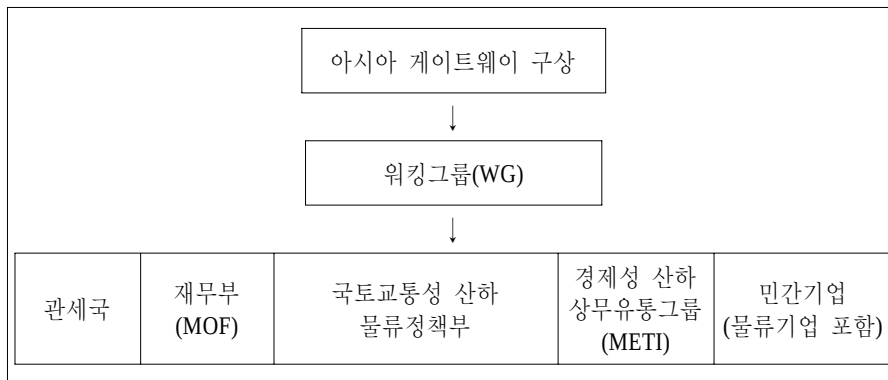
② 우리나라

우리나라는 대표적으로 물류보안 민관협의회를 통해 정부부처 간 협력을 모색하고 있다. 2007년 초에 발족된 동 협의회는 물류보안 현안에 대한 심도 있는 토의와 함께, 개별적으로 진행되고 있는 정부부처 간 물류보안 정책을 조정하기 위한 기능을 하고 있다. 하지만 비공식기구로서 아직 회의구성이나 운영에 있어서 보완해야 할 점이 많은 것이 사실이다. 따라서 일본에서 현재 운영되고 있는 워킹그룹이 이에 대한 시사점을 줄 수 있을 것으로 보인다.

일본정부는 올해 아시아 게이트웨이 구상(Asian Gateway Initiative)을 통해 세계 해양리더로서 발돋움하기 위한 장기플랜을 제시하고 있다. 이는 총 10개의 분야에 대해서 일본의 향후 전략을 구상한 것으로 물류보안과 관련해서는 2번째 주제인 ‘무역수속개혁 프로그램’에서 논의하고 있다. 동 프로그램의 주요 내용은 AEO 워킹그룹의 운영, 항만수속의 간소화, 특정수출신고제도의 혜택부여 및 일본판 AEO 제도의 구축 등으로 요약될 수 있다. 이 중 주목할 점은 일본정부가 이를 통해 개별조직을 강화하고, 각 부처 간 협력을 강화하고 있다는 사실이다. 물류보안을 담당하는 관세국, 재무부, 국토교통성 산하 물류정책부, 경제성 산하 상무유통그룹 등의 정부부처가 워킹그룹을 구성하고 이를 통해 협력을 이행하고 있다. 이 워킹그룹은 단기적으로 각 부처간 물류보안 관련 법률의 연계성을 높이는 데 초점을 두고 있다. 또한 올해 AEO 제도와 관련해 관세법이 개정된 바 있다.

<그림 4-2>

아시아 게이트웨이 구상에서의 부처 협력



자료 : 일본 국토교통성

한편 우리나라의 화물유통촉진법 전부개정 법률안(물류정책기본법)이 2007년 7월 국회를 통과하면서 2008년 1월부터 시행될 예정이다. 이 법안은 정부부처별로 추진되고 있는 물류정책을 효율적으로 조정할 수 있도록 추진체계를 정립하는 한편 국가물류정책위원회의 기능을 강화하고 국제적인 물류경쟁 환경 하에서 국내 물류기업의 국제경쟁력을 강화하기 위한 기반 구축을 주요내용으로 하고 있다. 동 법률의 주요조항⁶⁰⁾은 건설교통부장관 및 해양수산부장관의 협력가능성을 열어두고 있으며 특히 제11조에서는 양 부서가 공동으로 국가물류기본계획을 수립하도록 하고 있다. 동 법률에서 주목할 부분은 제17~19조에서 부처별로 분산되어 있는 물류정책기능의 효율적 조정 및 협조체제를 구축하기 위한 기구로 국가물류정책위원회⁶¹⁾를 설치·운영하도록 한 것이다. 이 위원회의 업무 사항은 이후 시행령 등에서 자세히 결정될 것으로 보이는데, 물류보안관련 AEO 제도의 협력, 국가물류보안체제구축과 관련한 협력에 있어 향후에 중요한 역할을 수행할 수 있을 것으로 기대되고 있다.

한편 ‘선박 및 항만시설 보안에 관한 법률’ 제7조 ③에서는 보안등급 설정 및 조정과 관련해 필요한 경우 국가보안기관 장의 의견을 구할 수 있고, 이에 국가기관의 장은 의견을 제시할 수 있도록 규정하고 있다.

나. 정부-민간 간 협력

빈틈없는 물류보안의 확보는 정부의 노력만으로 이뤄질 수 없다. 즉 민-관 협력 체제하에서 효과적인 물류보안이 확보될 수 있는 것이다. 예를 들어 대량살상무기의 경우 최종용도 및 최종사용자에 대한 정보는 일차적으로 기업에 의해 수집되기 때문에 통제당국과 기업간의 협력관계 강화가 중요하다.⁶²⁾ 따라서 민-관 협력체제 구축은 물샐틈없는 물류보안확보를 위해 필수조건이며, 현재 이러한 노력은 각국의 관세청을 중심으로 이뤄지고 있다. 이와 관련해서는 WCO의 세계 무역을 보호와 원활화를 위한 기준안(the Framework of Standards to Secure and Facilitate Global Trade : 이하 Framework)이 대표적이며, 이를 한 축으로 해서 미국의 C-T PAT, EU의 AEO제도, 스웨덴의 StairSec,⁶³⁾ 뉴질랜드의 SEP(Secure Exports Scheme Security

60) 제7,8조(물류현황조사), 제11조(국가물류기본계획의 종합·조정기능 강화), 제23조~26조(전진 물류체계의 구축), 제30조(국가물류 통합데이터베이스의 구축), 제59~60조(환경친화적 물류체계의 구축), 제61~63조(국제물류의 촉진 및 지원) 등이 대표적이다.

61) 법률에서는 국무총리 소속하에 국무총리를 위원장으로 하고 관련 중앙행정기관의 장 및 민간위원 등 24인 이내의 위원으로 구성하도록 하고 있음.

62) 이석기, “전략물자 수출통제와 관련된 기업인증제 실시 전망과 대책”(2006년 1월, KIET).

Plan)⁶⁴⁾ 및 싱가포르의 STP(Secure Trade Partnership)⁶⁵⁾와 같은 협력방안이 마련·시행되고 있다. 이 중에서 WCO와 더불어 미국과 EU에서의 협력현황을 살펴보도록 한다.

우선 WCO Framework⁶⁶⁾는 2005년 1월 WCO위원회에서 만장일치로 채택되었다. 이는 각 회원국 세관간의 협력(제1축)뿐만 아니라 세관과 민간기업간 협력(제2축)을 주요 두 축으로 구성되어 있다. 특히 세관과 민간기업간 협력은 AEO 제도를 통해 민간기업의 물류보안 책무를 강화하는 한편, 무역의 원활화를 위해 필요한 혜택을 부여하는 것을 골자로 하고 있다. WCO를 통한 세관과 민간의 협력구상은 “공급망 보안을 강화하고 국제무역의 흐름을 원활하게 하기 위한 WCO 회원국들과 민간산업간 협력방안 마련을 위한 가이드라인⁶⁷⁾의 선언⁶⁸⁾에 잘 나타나 있다.

63) 스웨덴은 통합물류보안 프로그램인 StairSec¹⁾을 통해 경제주체의 인증과 파트너십을 통해 민-관 협력을 수행하고 있으며, 이를 통해 통관을 위한 기업들의 비용을 76% 감소시켰으며, 세관의 적중률도 5%에서 45%로 높이는 효과를 가져왔음.¹⁾ 현재 StairSec은 스웨덴의 CSI 모델의 기반을 제공하고 있으며, 2003년 1월 고틀보르크항만(Port of Goeteborg)항이 이를 통해 CSI 인증을 받았음.

64) 뉴질랜드는 2006년 3월에 수출보안확보계획(Secure Exports Scheme Security Plan : SEP)을 수립하여 수출 분야에서의 보안확보를 위해 기업들과의 협력을 도모하고 있음. 이 계획의 핵심은 레드라인과 그린라인으로 구분된 세관절차임. 우선 그린라인의 지위를 획득한 기업에게는 최소한의 검색을 통한 절차간소화의 혜택을 제공하는 반면, 그린라인의 지위를 획득하지 못한 기업은 레드라인의 적용을 받아 엄격한 통관절차를 따라야 함.

65) 싱가포르는 최근 물류보안인증을 주요 내용으로 하는 민-관협력 프로그램을 내놓았음. STP 가이드라인이라고 불리는 프로그램을 통해 공급 업체들이 물류망의 보안을 확보하기 위한 요건¹⁾을 제시하고 이를 충족한 업체들에게는 싱가포르 세관이 STP 업체로 인증하게 됨.

66) WCO Framework의 이행과 관련해 동 협정 부속서에서 회원국 관세청이 ISCM 지침(WCO Customs guidelines on Integrated Supply Chain Management)에서 명시된 통합 관세통제절차를 준수하도록 규정하고 있음. 이후 ‘WCO 콜롬부스 계획(Columbus Programme)’이라 불리는 이행조치를 내놓았으며, 21세기 WCO 능력증진이사회(Capacity Building Directorate)가 이를 담당하고 있음. 한편, WCO의 주요 협약인 요하네스버그 협정과 양자협정도 이러한 협력조항을 포함하고 있음.

67) 영어 원명은 High Level Guidelines for Co-operative Arrangements between WCO Members and Private Industry to Increase Supply Chain Security and Facilitate the Flow of International Trade임.

68) “공급망에서의 위협을 평가하고 해결하기 위해 무역에 종사하는 파트너들과 얼마만큼 협력관계를 맺는가에 따라 세관이 직면하고 있는 위협의 감소수준이 달라짐. 따라서 공급망 보안을 강화하고자 하는 의지를 명백히 하는 기업들은 혜택을 누릴 수 있음. 이러한 방법으로 리스크를 최소화함으로써 세관당국은 고유의 보안기능을 수행하고 합법적 무역을 촉진시킬 수 있음(To the extent that Customs can rely on its partners in the trade community to evaluate and address threats to their own supply chain, the risk confronting Customs is reduced. Therefore, companies that demonstrate a verifiable willingness to enhance supply chain security will benefit. Minimizing risk in this way helps Customs in performing their security functions, and in facilitating legitimate trade.).”

<표 4-2>

WCO 세관-민간 협력 주요 내용

기준 (Standard)	주제	구체적 내용
기준 1	파트너십	• AEO의 기존 보안기준과 최적관행(Best Practice)에 근거한 자기평가(self-assessment)
기준 2	보안	• AEO의 민간사업영역의 보안최적관행의 준수
기준 3	인증	• AEO 인증절차 및 혜택부여 절차
기준 4	기술	• 최신 기술을 사용을 통해 화물과 컨테이너의 보안확립을 위한 주체의 노력
기준 5	의사소통	• 최소한의 보안기준과 최적관행을 수립하기 위한 세관-민관 파트너십 프로그램의 업데이트
기준 6	무역 원활화	• 세관과 AEO간 무역원활화를 위한 협력

자료 : WCO Framework

미국의 경우, 민-관 협력은 C-T PAT(the Customs-Trade Partnership Against Terrorism)⁶⁹⁾에 잘 나타나 있는데, 이는 2001년 9.11테러 이후 민관협력을 통한 물류보안구축을 위해 도입되었다. C-T PAT은 자발적 참여를 원칙으로 하며 대량살상무기를 포함한 테러무기의 반입을 저지하는 동시에 물류 망의 안전을 도모하기 위해 미국 세관국경보호국(CBP), 국토안보부(DHS)와 민간기업의 협력을 골자로 한다. 구체적으로 미국으로 들어오는 화물에 대한 보안을 강화하면서 C-T PAT의 조건을 충족하는 기업에게 혜택과 인센티브를 제공한다. 따라서 C-T PAT은 화물 보안을 강화함으로써 발생하는 물류기업들의 비용을 인센티브의 제공을 통해 완화함과 동시에 화물의 통관을 용이하게 하여 궁극적으로 무역원활화를 지향한다. 이와 함께 미국 SAFE Port Act Sec.236는 민간부분과 물류보안 관련 정보공유를 위한 연락소 설립 및 효율적인 정보공유 체제 구축을 마련하도록 하고 있으며, 이를 위해 통상운영자문위원회(Commercial Operations Advisory Committee)와 협의하도록 규정하고 있다.

한편 EU는 2007년 5월 발표한 AEO 가이드라인 Ⅲ.8에서 세관당국과 AEO기업간의 협력을 증진하기 위해서 기업이 세관에 대한 접근성을 높이고 연락을 원활하게 하기 위한 서비스 센터를 설립할 것을 명시하고 있다. 또한 CSP(Customs Security

69) 초기에는 7개의 주요 수입업체를 대상으로 시작하였지만, 지금은 외국기업을 포함해 물류산업에 종사하는 약 7,500여개 기업이 등록되어 있음.

Programme)에 따라 국제 공급망 보안을 위해 세계 주요 민간 무역업자와의 긴밀한 협력관계를 구축하고 있다.

다. 양자협력

① 국외사례

현재 물류보안에 대한 인식이 확산되면서 국가 간 협력기반이 확대되고 있다. 이러한 국가 간 협력은 크게 양자협력과 국제기구에서의 협력을 포함한 다자협력으로 나뉘지는데, 이 중 양자협력이 EC와 미국 등을 중심으로 눈에 띄게 증가하고 있다.

우선 EC는 무역파트너와 물류보안확립을 위한 양자협력을 적극적으로 모색하고 있다. EC-중국간 양자협력의 경우, 보안절차 및 방법에 대한 상호인정 및 상호주의(reciprocity)를 중심으로 물류보안협력을 이행하고 있다. 이를 위해 2006년 9월 19일 합동 세관협력 위원회(Joint Customs Co-operation Committee)가 출범하였다. 이 위원회는 우선 네덜란드 로테르담 항, 영국의 펠릭스토우 항, 중국의 선전항을 중심으로 해상 컨테이너 보안을 강화하기 위한 시범사업을 실시하고 있다. 이러한 시범사업이 성공한다면 이를 EC 전체 항만으로 확대하는 계획을 세우고 있다.

미국은 물류보안 선두주자인 만큼 양자협정을 통한 물류보안 강화에 힘쓰고 있다. 일례로 멕시코와 캐나다와 함께 FAST(The Free&Secure Trade Program)을 통한 협력을 이행하고 있는데, 이는 화물의 국경이동시 보안확보와 원활한 통관을 위한 것이다. 이는 기준에 적합하다고 사전 승인된 화물이 국경을 통과하는 경우 신속하고 간소화된 절차를 적용하는 것을 골자로 한다. 한편 EC와는 호혜주의를 바탕으로 보안기준의 상호인정 및 비즈니스 공동협력 프로그램을 위해 노력하고 있으며 AEO와 C-T PAT간의 상호 인정을 위한 노력을 지속하고 있다. 그리고 9.11 이행법 Sec.711은 비자면제와 관련해서 반테러 및 정보공유를 위한 양국간 협력을 강조하고 있다. 특히 Sec.1842는 대량살상무기와 관련해 러시아와의 공조를 규정하고 있다.

한편 오세아니아 지역에서도 이러한 협력이 활발히 이뤄지고 있다. 우선 뉴질랜드 관세청은 2005년 11월 중국 베이징에 새로운 관세사무소(Customs Post)를 세워 교역증대로 인한 양국간 세관문제를 해결하고 있으며 특히 중국과의 FTA 이행을 지원하고 있다. 또한 오세아니아 세관기구(Oceania Customs Organization : OCO)의 지원

을 통해 태평양지역의 세관활동을 강화하면서 국경보안과 무역 원활화를 위한 협력을 강화하고 있다. 호주의 경우 프론트라인(Frontline) 계획을 통해 세관과 민간 협력을 강화하고 있는데, 민간업체에 대한 교육을 주된 사업으로 하고 있다.

이렇듯 양자협력은 현재 주로 경제협정체결에 따른 협력의 필요성 및 물류보안 시범사업의 공동이행 등을 중심으로 이뤄지고 있다.

② 우리나라

우리나라의 양자협력의 경우는 크게 관세청을 중심으로 한 AEO 상호인증제도의 마련을 위한 시범사업의 추진과 FTA 체결이행을 위한 물류보안협력 틀 마련을 통해 이뤄지고 있다.

우선 우리나라 관세청은 현재 국제적인 물류보안강화 논의 및 흐름에 적극 대응하기 위해 내적으로는 WCO의 세관 데이터 모델(CDM) 및 화물고유번호(UCR) 체제에 부합하는 세관정보교환 및 화물관리시스템의 도입 기반을 조성하는 한편, 외적으로는 WCO의 SAFE Framework의 이행을 위한 세부계획의 마련에 적극 참여하고 벨기에, 필리핀 등과 세관정보교환 및 물류보안에 관한 시범사업을 추진하는 등 국제적인 협력을 강화하고 있다. 특히 AEO 제도의 국가 간 상호 인증과 관련해 벨기에 관세당국과 통관정보교환 및 화물보안 시범사업을 공동으로 추진하고 있다. 또한 지난 9월 필리핀 마닐라에서 필리핀 관세청과 통관정보 교환 시범사업 추진을 위한 양해각서(MOU)⁷⁰⁾를 체결하였다.

현재 진행 중인 한-EU FTA 협정체결과정에서 통관분과에서 통관 원활화(Trade Facilitation) 협정문에 물류보안관련 협력에 관한 조항삽입을 검토하고 있는 것으로 알려졌다. 이는 EU측이 제안한 것으로 크게 1) 양 국간 세관협력, 2) 양 국간 물류보안 관련 다자 포럼에서의 입장 조정을 위한 협력 등의 내용으로 구성되어 있다. 우리나라 정부는 이와 관련해서 단순협력사항에 대한 내용이므로 이를 수용할 것으로 알려지고 있다. 하지만, 양국간 FTA 협정에 물류보안관련 협력조항이 삽입되고 있는 것만으로 양자간 협력을 위한 토대는 마련되었다는 의의가 있다.

한편 ‘선박 및 항만시설 보안에 관한 법률’ 제9조(대체보안협정)에서 해양수산

70) 이번 시범사업을 통해 한국과 필리핀 관세당국은 세계관세기구(World Customs Organization, WCO)에서 권고하고 있는 30여종의 수출화물 정보를 사전에 교환하게 되며, 교환된 정보를 바탕으로 수입물품이 입항하기 전에 위험물품만을 선별하여 검사하고 나머지 물품은 신속하게 통관해 주는 한편, 한번 제출한 항목은 다시 제출하지 않도록 하기 위한 글로벌 통관단일창구(Single Window) 프로젝트를 시범적으로 운영할 계획이다.

부장관이 고정된 단거리 국제항행에 취항하는 선박이 기항하는 항만의 당사국 정부와 대체보안협정을 체결할 수 있도록 하고 있다.

라. 다자협력

① 국외사례

다자협력은 국가 간 사안에 대한 합의를 도출하고 이를 통해 협력을 확산시킨다는 의미에서 가장 바람직한 협력방안으로 여겨진다. 반면 국가 간 이해가 상충하는 문제의 경우 오히려 다자협력의 모색은 문제해결을 오히려 더디게 할 수 있다. 현재 국제사회에서 이뤄지는 다자협력은 지역 국가 간 새로운 협의체를 구성하기보다는 주로 기존의 협의체를 통해 물류보안 의제를 다루는 방식을 채택하고 있다.

시각을 지역으로 돌려보면 우선 아·태 지역에서는 APEC이 물류보안 다자협력을 선도하고 있다. APEC의 물류보안 가이드라인은 회원국들에게 물류보안확보를 위해 자국의 공급자와의 의사소통(communication), 위협평가(assessment) 및 이에 대한 교육(training)을 강조하고 있으며, 특히 공급자와의 협력을 위해서 인센티브를 제공할 것을 권유하고 있다. EU의 경우 DG TREN 워킹그룹(Commissions' Directorate-General Transportation and Energy Working Groups)에서 IMO, ICAO 및 IAEA와 같은 국제기구와의 다자적 협력⁷¹⁾을 모색하고 있다.

미국은 항만보안법(SAFE Port Act) 및 9.11 테러대책 이행법률을 통해서 다자협력의 근거를 수립하고 있다. Sec.404는 1930년 관세법(Tariff Act of 1930) Sec.629를 개정하면서 국토안보부, 국무부와 기타 관련 정부기관들이 WCO, WTO, IMO 및 APEC을 포함한 관련 국제기구들과 세관절차, 표준, 요건 등에 관련해 국제무역 촉진화를 위한 협력을 하도록 규정하고 있다. 또한 Sec.122는 해외에서 미국으로 들어오는 카페리선 검색과 관련해 카페리선사뿐만 아니라 적절한 해외 정부기관과의 협력 하에 검색계획을 마련하도록 하고 있다.

또한 9.11 테러대책 이행법 Sec.1101은 대량살상무기거래 및 방지와 관련해 국가 생물감시 통제센터(National Bio-surveillance Integration Center : NBIC)를 지원하기 위한 정부기관 간 협력을 촉진하기 위한 워킹그룹설립을 규정하고 있으며,

71) 이러한 협력은 주로 1) 운송 및 수송망에 대한 보안문제 이해 증진, 2) 국가의 최적 관행(best practice)의 발굴 및 경험의 상호교환, 3) 보안의 최적관행을 중심으로 한 관행의 표준화를 위한 발전 모색, 4) 상호 인증된 보안방법을 통해, 상호주의를 기반으로 화물과 승객보안에 대한 상호협정의 체결 등임.

Sec.1821은 대량살상무기 확산방지구상(PSI)관련해서 모든 국가(all countries)와의 협력을 강화하며, PSI 참여국가 간 조정, 협력 및 이행을 담당할 다자적 기제(mechanism)를 마련하도록 하고 있다. Sec.1852~1859는 대량살상무기 및 테러확산 방지 위원회(Commission on the Proliferation of Weapons of Mass Destruction and Terrorism)를 설립해 국제기구와 다른 국가와의 협력을 위원회의 의무로 규정하고 있다. Sec.1901은 반테러리즘 기술관련 국제사회 협력을 규정하고 있는데, 이를 위해 국토안보부 장관은 과학기술 국토안보 국제협력 프로그램 사무소(the Science and Technology Homeland Security International Cooperative Programs Office)를 설립하도록 하고 있다. Sec.1841은 대량살상무기(WMD) 확산방지를 위해 국제사회와의 협력을 통해 법과 제도의 개선을 모색하고 있으며, 나아가 보편관할권(Universal Jurisdiction)을 도입해 모든 국가들이 속지주의 및 속인주의의 제한을 받지 않고 대량살상무기관련 범죄자를 처벌할 수 있도록 국제사회와의 유대를 강조하고 있다. 이 법률과 관련해 주목을 끄는 부분은 우선 파키스탄, 아프가니스탄 및 사우디아라비아와의 협력을 조문으로 명시하고 있어 이 국가와의 협력을 중요하게 여기고 있다는 사실이다. 또한 테러방지 및 근절을 위해서는 민주주의 확산이라는 정치적 이데올로기의 강화가 필요하다는 인식하에 국제기구 및 지역기구(EU, AU 및 NATO), 유럽 및 아시아 민주주의 국가와의 지속적인 교류 및 협력을 모색하고 있다는 사실이다.

② 우리나라

‘선박 및 항만시설 보안에 관한 법률’을 보면 제5조(국가항만보안계획 등) ②-8에서 국가항만보안계획에 항만시설보안에 관한 국제협력의 사항을 포함하도록 규정하고 있으며 제6조(보안위원회 설치 등) ②-4에서 보안위원회의 심의·조정 대상에 선박 및 항만시설의 보안과 관련되는 국제협력에 관한 사항을 규정하고 있다. 또한 위와 같은 명시적 협력조항 이외에 제11조에서 해양수산부장관은 대한민국 선박 및 항만시설의 보안에 관해서 해양수산부령이 정하는 사항을 국제해사기구에 통보하도록 하는 의무규정을 두고 있다.

또한 지난 해 9월 서울에서 개최된 한·중·일 물류장관회의에서는 의제 중 하나로 물류보안 협력을 다루었다. ‘물류보안의 확보와 물류 효율화의 양립’이라는 의제를 통해 당사국들은 해상운송에서의 전자 태그 등을 활용한 시범사업 및 각국의 물류보안의 확보, 물류 효율화를 위한 정보공유와 안전하고 효율적인 물류시스

템의 구축을 위한 의견교환 등을 합의하였다. 이는 구속력 없는 선언적인 수준에 그쳤다 하더라도 물류보안 협력에 대한 3국의 관심과 의지를 표명한 것으로 향후 물류장관회의를 통해 협력을 확대·강화할 수 있는 기반을 다진 것으로 평가할 수 있다.

(3) 우리나라의 제도 확립 방안 : 다층적 전략⁷²⁾

앞서 살펴본 바와 같이 물류보안 협력은 물류보안 인식이 확대되면서 다층적으로 이뤄지고 있다. 즉 물류보안 협력은 크게 정부-정부, 정부-민간 및 민간-민간분야에서 이뤄지고 있다. 정부-정부의 협력은 최근의 미국과 멕시코 및 캐나다의 무역보안 프로그램(Free&Secure Trade Program) 등의 양자협력과 APEC 등에서 이뤄지고 있는 다자협력으로 나뉘고, 민간-정부의 협력은 현재 가장 활발하게 논의되고 있는 분야로 C-T PAT, AEO 제도 등이 이에 속하고 있다. 한편 민간-민간의 협력은 그 필요성에 비해 현재 다른 분야와 비교해 아직 활성화되고 있지 않으며 주로 기술적 협력에 국한되고 있는 특징을 보여주고 있다⁷³⁾. 이와 관련해 양 국간 물류보안 상호인증제도는 정부-민간-정부의 새로운 협력의 양태를 띠고 있어 주목을 끌고 있다. 미-EU의 물류보안 상호인증제도⁷⁴⁾ 등이 이에 해당되는데, 이러한

72) 국제협력은 크게 국가 간 양자협력과 국제기구 및 협의체를 통한 다자협력으로 나뉘 살펴볼 수 있음. 이러한 양자협력과 다자협력의 가장 큰 차이점은 구속력(binding power)과 합의(consensus)라는 요소로 살펴볼 수 있음. 즉 양자협력의 경우 구속력은 높으나 또한 쉽게 파기될 수 있는 위험성이 높은 반면, 다자협력은 국가를 구속하는 구속력은 상대적으로 낮으나, 합의(consensus)를 통해 일단 협력이 성립되면 쉽게 파기될 수 없는 특성을 지닌다고 볼 수 있음. 따라서 이 둘 간의 적절한 조화를 통한 다층적 협력방안을 추구하는 것이 협력을 통해 도달하고자 하는 목표에 근접할 수 있을 것임.

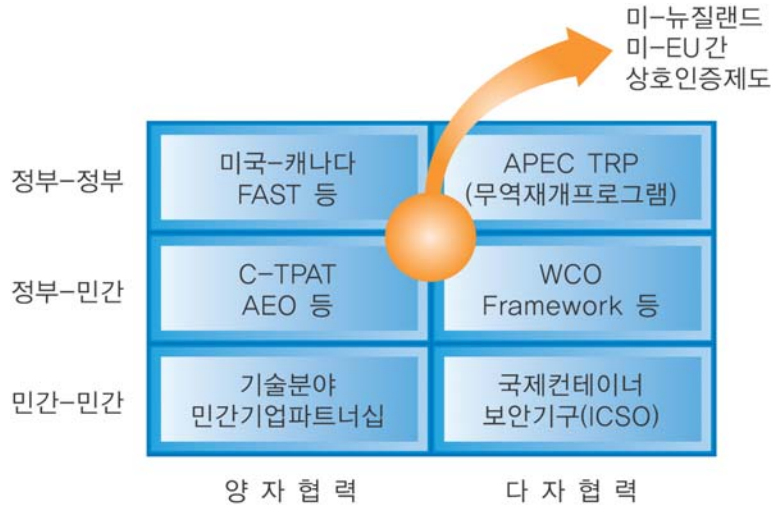
73) 11월 두바이에서 개최된 Container Tracking & Security 2007에 참여한 기업대표들은 개별적으로 개발하고 있는 보안장치에 대한 국제적 기준이 마련되어 있지 않아 문제가 되고 있다고 지적하고, 통일된 기준마련에 협력해야 한다는 데 뜻을 같이 했음. 한편 이번 세미나에서는 미국 CBP, 유럽위원회 및 디퍼월드, 허치슨 터미널, IBM, SAVI 등 물류보안 관련 정부기관과 민간기업 관계자가 참석해 물류보안에 대한 높은 관심을 반영했음. 이번 세미나는 물류보안 기술 및 제도분야 현황과 관련이슈를 이틀에 걸쳐 전반적으로 다루었으며 특히 홍콩, 사우스햄튼, 암스테르담항의 항만보안 사례와 IBM, Sony사 등 기업들의 사례가 소개되어 눈길을 끌었음. 이번 세미나에서는 컨테이너 보안장치의 표준화 문제, 미국 주도의 100% 컨테이너 화물 검색법과 WCO Framework의 조화 가능성 등에 대해 좀 더 심층적인 논의가 필요하다는데 의견을 같이 했고, 이를 위해서는 향후에도 민간 차원에서 적극적으로 자신들의 목소리를 내어야 하며 정부도 관심을 가지고 민간과 지속적인 협의를 해야 한다는데 의견을 같이 했음.

74) 최근 우선 미-EU간 제 1차 대서양 경제이사회(Transatlantic Economic Council : 이하 TEC)에서는 물류보안협력을 위한 상호인증이 주요 의제 중 하나로 논의되었음. 이번 TEC 1차 회의에서는 미국의 반테러 민-관 협력 보안제도인 C-T PAT(Customs-Trade Partnership Against Terrorism)과 EU의 승인된 경제 운영자(Authorized Economic Operator) 제도의 상호인증문제가 주요 이슈였음. 이는 양국의 C-T PAT 및 AEO에서 제시한 기준을 충족한 기업에 대해 양 국이 부여하고 있는 세관절차 간소화 혜택 등을 부여할 수 있도록 하는 것을 주요 골자로 하고 있음. 이는 유럽의 AEO로 인정된 기업이 미국에서

협력의 추세가 앞으로도 지속될 것으로 보이고, 현재 싱가포르의 물류보안 계획인 STP(Secure Trade Programme)도 타 국가와의 물류보안 상호인증을 목표로 시행되고 있다.

<그림 4-3>

물류보안 협력 다층적 구조도



자료 : 한국해양수산개발원

우리나라 물류보안 협력과 관련해 주목해야 할 점은 국내에서의 협력이 국제협력보다 상대적으로 미약하게 이뤄지고 있다는 것이다. 이는 물류보안의 이슈가 주로 항만을 중심으로 국가 간 이동하는 화물에 초점이 맞춰져 있어 국민적 컨센스가 아직 이뤄지고 있지 않기 때문인 것으로 파악된다. 앞서 살펴본 대로 우리나라는 물류보안 민-관 협의회를 구성해 정부 간 협력뿐만 아니라, 민-관 협력체제

도 동일하게 인정되어 별다른 조치 없이 미국이 C-T PAT 기업에게 부여하는 혜택을 받을 수 있게 되는 것을 의미함. 나아가 미국과 EU 회원국은 세관보안 관계자를 교환 파견하여 양국의 보안절차 및 세관보안 시스템을 학습할 수 있도록 하는 방안을 선행조치로서 내놓았음. 일례로 EU 관계자가 국경세관 보호국(Customs & Border Protection : CBP)의 NTC(National Targeting Center)에 파견되어 컨테이너 화물 검색 및 선적정보 분석에 대해 교육받게 될 것이고, 2008년에는 CBP와 EU가 인증기업에게 적용하는 절차 등과 관련한 합동 검증업무(Joint Validation)를 수행할 것으로 알려졌다. 한편 이번 대서양 경제이사회에서의 수확은 서로 다른 입장차이 및 해결해야 할 문제에도 불구하고 물류보안 협력에 한 목소리를 내었다는 것임. 실제로 미국 CBP의 기준이 EU AEO의 기준보다 엄격한 것으로 알려졌는데, 이러한 양 당사자간 상호인증 기준이나 방식의 차이가 향후 해결과제로 대두되었음. 하지만, 미국과 EU는 양국 물류보안 상호인증을 위한 로드맵을 위해 향후에도 지속적으로 협력할 것을 약속하였음. 이는 미-EU의 경제교류 및 발전을 위해서는 무역의 안전이 중요하며 이를 위해 지속적인 협력이 필요하다는 공감대가 형성되었기 때문임.

구축을 도모하고 있지만, 상설 협력체로서 위상을 지니기 위해서는 여전히 해야 할 일이 산재해 있다. 그리고 무엇보다도 대국민 인식이 부족해서 사회적 공감대를 형성하는 데도 성과를 내지 못하고 있는 실정이다.

이러한 측면에서 볼 때 상대적으로 국제협력은 활발하게 이뤄지고 있는 것으로 보인다. 우선 관세청이 벨기에와 필리핀이 추진하고 있는 AEO 시범사업의 사례와 올해 초부터 APEC TRP(Trade Recovery Programme)에 정부 대표단을 파견해 아-태 지역의 물류보안 레짐 형성에 지속적으로 의견개진을 하고 있는 것은 정부차원에서 물류보안에 대한 인식이 점차 나아지고 이를 통한 협력의 토대가 구축되어가고 있다는 반증으로 보인다. 또한 한-EU FTA의 협상과정에서도 물류보안을 하나의 의제로 포함시킴으로써 양국간 협력근거를 마련한 것도 이러한 성과 중 하나로 볼 수 있다. 그리고 관세청 및 산업자원부 기술표준원을 중심으로 WCO나 ISO의 물류보안 관련 국제규범 제정에 지속적으로 참여하고 있는 것도 국제협력에서 이니셔티브를 잡기 위한 의미 있는 성과로 보인다.

그렇다면 이러한 현황에서 향후 우리의 협력방안은 어떠해야 하는가? 답은 간단하다. 즉 국내협력과 국제협력의 유기적인 조화를 통해 다차원적 협력체계를 구축해야 한다는 것이다. 하지만, 실천적인 측면에서 보면 이는 간단하지만은 않다. 그 이유는 물류보안이라는 것이 무역의 원활화와 안보라는 협력의 과제를 던지는 이면에 물류보안시장에서의 자국 이익확보라는 경쟁적인 과제도 함께 제시하고 있기 때문이다. 따라서 자국의 물류보안기업의 경쟁력도 확보하면서 국내외적 협력을 구축하는 윈-윈 전략이 필요할 것으로 보인다.

이를 위해 국민들의 공감대 형성을 전제로 하여 정부 부처간 물류보안 법령정비를 위한 협력이 필요하며, 현재 운영중인 물류보안 민관협의회가 활성화되어야 한다. 이러한 국내협력을 바탕으로 양국 간 물류보안 상호인증 시범사업을 추진하고, FTA와 같은 경제협정에 물류보안 협력규정을 삽입하여 양국간 협력근거를 마련하여야 한다. 그리고 한중일 3국간 물류장관회의를 통해 동북아 물류보안 협력 활성화를 꾀하고 이를 통해 국제사회의 물류보안 이니셔티브를 행사할 수 있도록 해야 한다. 마지막으로 WCO, IMO 및 ISO 등 물류보안 관련기구의 규범화 작업에 지속적으로 참여해 국제규범의 제정이 국내에 미칠 수 있는 영향력을 최소화하고 나아가 이를 통해 국익을 추구할 수 있도록 해야 한다.

<그림 4-4>



자료 : 한국해양수산개발원

2. 물류보안 인프라 구축 및 전문인력 육성

1) 물류보안 하드웨어 인프라 구축

물류보안 인프라체제를 크게 보면 물류보안 협력을 포함한 제도 부분과 기술적인 분야로 나눌 수 있다. 기술적인 분야도 크게 장비 및 장치를 제조하여 판매하는 하드웨어 부분과 하드웨어 운영에 수반되는 각종 정보를 처리 분석하는 소프트웨어와 솔루션 및 보안관련 서비스 컨설팅 분야 등으로 나뉘 살펴볼 수 있다. 이 중 기술적 분야에서의 하드웨어 인프라에 초점을 맞춰 구축방안에 대해 살펴보도록 한다.

(1) 물류보안 하드웨어 인프라 시장

현재 물류보안 하드웨어 인프라 시장은 가히 폭발적으로 성장하고 있다. 앞서 언급된 스마트 컨테이너 시장의 경우 2006년 약 7,000만 달러에서 2012년에는 약 42억 달러로 예측되고 있다. 또한 2003년 HSRC(Human Science Research Council)의 예측에 따르면 미국 컨테이너 검색기 시장의 규모는 2002년 7,000만 달러에서 2010년 4억 4,000만 달러로 약 650% 성장할 것으로 전망되었다. 그리고 이러한 물

류보안산업은 글로벌 물류기업이 선점하고 있다. 보안솔루션과 관련된 글로벌 기업의 시장 지분 확보 전략은 이와 함께 점점 더 치열해지고 있다. SAVI는 선도적인 원천기술 개발로 국제표준을 이끌며 시장 지분을 확보하려는 전략을 펴고 있으며 구체적으로는 국제 공동 프로젝트에 참여하여 단체 표준기술로 확정된 후 이를 상품화하고 있다. 또한 GE의 경우 인수·합병을 통한 기술흡수 후 기존 시장에 영향력을 확보하려 하고 있다.⁷⁵⁾

이러한 물류보안 하드웨어 시장은 최근 발표된 미국의 9·11 Commission Act of 2007(일명 100% 화물검색 법)에 의해 더욱 확대되고 있다. 최근 자료에 따르면 초고속 검색시스템을 기준으로 그 수요가 크게 늘 것으로 전망되고 있다. 우리나라의 경우 2006년 기준으로 대미 컨테이너 검색 필요량은 TEU로 140만 개였으며, 2012년까지 평균 물동량 증가율을 20%로 예상할 경우, 검색이 필요한 컨테이너는 420만개에 달하게 된다. 이를 필요한 초고속 컨테이너 검색기로 환산하면 현재 필요한 초고속 검색시스템의 개수는 42대에 이르며 금액으로는 1조원에 해당된다. 만약 100% 검색법이 발효하여 미국으로 가는 모든 화물(환적화물 포함)에 대한 사전 검색이 강화된다면, 세계적으로 컨테이너 검색기 시장의 규모는 더욱 커질 것이 분명하다.

<표 4-3>

초고속 컨테이너 검색기 특징

구분	기준 정속 컨테이너 검색기	초고속 컨테이너 검색기	선진국대비 국내 기술 개발 수준(%)
X-ray 발생기술	9MeV	6MeV	20
처리시간(대/시간)	20	100	40
검출 기술	16bit	16bit	90
영상처리 기술	1mm	12mm	90
투과력	400mm	300mm	90
설치 비용	100억	30억	60

자료 : 2007 국제 물류보안 동향 및 대응전략 세미나 자료

이러한 시점에서 우리나라의 물류보안 과제는 인프라 구축을 통해 물류보안이라는 실질적 이득을 목표로 하는 동시에 물류보안 시장경쟁력을 강화하는 것이다. 이를 염두에 두고 인프라 구축방안에 대해 살펴보도록 한다.

75) 2007년 국제 물류보안 동향 및 대응 전략 세미나 자료집 참조.

(2) 인프라 구축방안

서두에서 언급한 바와 같이 컨테이너 보안장치 시장이 커지면서 더 큰 파이를 차지하려는 기업들의 경쟁이 치열하게 이뤄지고 있다. 여기에 삼성물산 등 국내기업도 주도권을 잡기 위한 전략적 행보를 가속화하고 있다. 따라서 컨테이너 보안장치 관련 인프라 구축은 이러한 현황을 염두에 두고 논의되어야 한다. 이와 관련 인프라 구축방안을 크게 공감대 형성, 기술 연구개발, 기술 부분 투자활성화와 이를 뒷받침할 수 있는 제도적 지원 등으로 나눠 살펴볼 수 있을 것이다.

가. 인프라 구축에 대한 공감대 형성

우선 공감대 형성 측면에서 물류보안에 대한 인식의 확산이 전제되어야 한다. 이는 정부와 기업뿐만 아니라 화주들에게 특히 요구되는 부분이다. 최근 두바이에서 개최된 Container Security&Tracking 2007에서 기술 분야 참여자의 대부분도 이러한 점에 대한 불만을 토로하였다. 즉 보안장치의 도입에 대한 정부의 지원이 이뤄지지 않는 가운데, 컨테이너 보안장치에 대한 실질적 수요자인 화주가 이와 같은 장비의 도입을 비용 상승의 주범으로 보고 있기 때문이다. 이로 말미암아 보안장치에 대한 인식의 제고는 여전히 보안장치 개발 기업을 중심으로 이뤄지고 있으며, 화주를 포함한 전 부분의 주체들 모두가 동일한 공감대를 형성하고 있지 못하다.

한편 정부차원에서 이러한 공감대 형성을 위한 적극적 홍보에 나서고 있지 않은 것도 문제로 지적될 수 있다. 현재 물류보안 민·관 협의회가 운영되고 있지만, 협의기구의 성격으로 인해 여전히 추진력 있는 정책발굴이나 홍보활동을 하고 있지 못하고 있는 것으로 알려지고 있다. 이와 더불어 정부 부처 간에도 이렇다할 협력이 이뤄지고 있지 않으며, 기술 관련 주무부서라고 할 수 있는 과학기술부에서도 적극적인 정책을 제시하고 있지 않은 것으로 알려지고 있다. 물론 각 부처에서 물류보안과 관련해 부처별 정책을 제안·실시할 예정인 것으로 알려졌다.

따라서 인프라 구축을 위한 시발점은 이러한 공감대 형성으로부터 출발하여야 한다.

나. 기술 연구개발(R&D)지원

전자봉인의 경우 기본적으로 1회성의 소모품 성격을 띠고 있기 때문에 엄청난 시장잠재력을 가지고 있을 것으로 판단된다. 모든 컨테이너에 1회성 전자봉인이 부착될 경우 40피트 컨테이너를 기준으로 약 2억여 개의 전자봉인이 소모되

게 된다. 따라서 전자봉인 분야는 기술 연구 및 개발을 통해 향후 막대한 수익을 거둘 수 있는 영역으로 판단된다. 이는 R&D 추진을 서둘러야 하는 주요한 이유이다.

<표 4-4>

세계 컨테이너 처리량 및 수송량 추이

구 분	컨테이너 처리량		세계 컨테이너 수송량	
	물동량(백만TEU)	증가율(%)	물동량(백만TEU)	증가율(%)
2003	316.8	14.2	91.9	14.7
2004	363.7	15.4	105.4	14.7
2005	400.6	10.1	115.9	9.7
2006	441.9	10.3	127.7	10.2

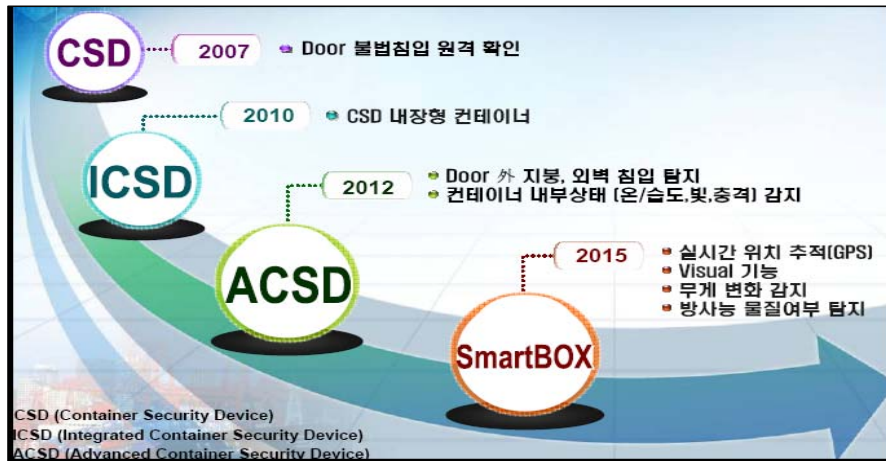
자료 : Drewry Shipping Consultants Ltd, Annual Container Market Review and Forecast 2006/07

스마트 컨테이너의 경우 그 시장규모는 전자봉인보다는 작을 것으로 추산된다. 부착되는 각종 장비나 향상된 보안성으로 인해 대규모의 시장보다는 화학산업, 군수산업, 고가산업(귀금속, 반도체 웨이퍼운송) 등의 전문화된 분야에서 가능성이 높을 것으로 판단된다. 이러한 스마트 컨테이너의 경우에는 전자봉인보다 IT 시스템과의 연계가 더욱 필수적으로 요구된다. 이 점은 IT강국인 우리나라 기업이 강점을 보일 수 있는 부분이다. 특히 스마트 박스를 구성하는 시큐리티 장치, 센서와 더불어 GPS를 활용한 구간별 위치 및 파손가능성에 대한 정보를 실시간으로 보내는 물류 Tracking서비스는 고도의 IT기술을 기반으로 하고 있다. 따라서 최첨단 정보통신 기술을 보유한 우리나라로서는 이를 바탕으로 스마트 컨테이너를 업그레이드시키는 기술개발이 필요할 것으로 보인다.

한편 이러한 기술 연구 및 개발의 주체는 어느 한 분야의 주체가 주도해 나가기 보다는 민-관 파트너십에 의한 접근이 보다 효율적일 수 있다. 우선 정부는 물류보안산업의 육성책으로 정책을 수립하고 이를 토대로 예산을 확보하여 연구소를 통한 기술 개발뿐만 아니라 경쟁력 있는 기업에 적극 지원을 할 수 있다. 기업의 입장에서는 자체 내 최첨단 기술을 개발하는데 필요한 자금을 정부로부터 지원받으며 개발로 인한 위험을 상당부분 보증 받을 수 있다. 이 가운데에서도 기술개발은 민간기업, 재정적 지원은 정부가 제공하는 민-관 파트너십에 의한 R&D 사업추진이 바람직하다.

<그림 4-5>

컨테이너 보안장치(CSD) 로드맵



자료 : 국제 물류보안 동향 및 대응방안 전략 세미나(2007)

다. 기술표준부분 이니셔티브 확보

기술 분야 인프라 구축과 관련해 빼놓을 수 없는 또 하나의 이슈는 바로 표준화 문제이다. 전자봉인의 경우 국제표준으로 듀얼밴드가 사실상 확정됨에 따라 생산 원가의 상승에 따른 가격인상으로 전체적 시장 규모의 축소에 대한 우려가 있는 반면 시장외적인 강제규정과 전수검사에 대한 불이익 등을 고려하면 영향을 받지 않을 것이라는 관측도 존재한다. 따라서 보다 수준 높은 기술 개발을 통해 원가를 낮추면서 동시에 듀얼밴드를 지원하는 장비를 개발하는 것을 고려해 볼 수 있다.

앞서 언급한 바와 같이 국제표준기구(ISO)를 통해 컨테이너 전자 봉인 표준이 433MHz와 2.45GHz 주파수를 모두 지원하는 방향으로 확정됐다. 그리고 전자봉인장치와 관련해서는 ISO 18185, 공급사슬관리 보안은 ISO 28000시리즈를 통해 구체화되었다. 미 국토안보부도 조만간 컨테이너 보안장치 요건을 제시할 것으로 알려지고 있다. 그 요건에 대해서는 많은 논란이 있지만, 전문가들은 이번 국토안보부의 표준도 ISO 표준을 기본적으로 따를 것으로 보고 있다. 하지만 이러한 전자봉인을 포함한 보안장치 관련 표준화 과정에서 우리의 입장정리가 아직은 없는 것으로 보인다. 특히 세부적 기술 분야에서의 표준작업이 앞으로 지속적으로 이뤄질 것이라고 가정하면 분야별 표준작업 가능성을 타진하고 우리의 입장을 정리하는 작업이 필요할 것이다. 이는 기술연구 및 개발의 결과와 직결되는 중요한 사안이기 때문이다. 즉 우리가 개발한 장비 및 기술이 국제적인 표준으로 자리 잡는다면 이러

한 이니셔티브를 통해 시장지분을 지배적으로 확보할 수 있지만, 반대로 장비 및 기술을 보유하고도 이후 국제적 표준은 이와 상이하게 제정된다면 그간의 노력은 물거품이 될 가능성이 높기 때문이다.

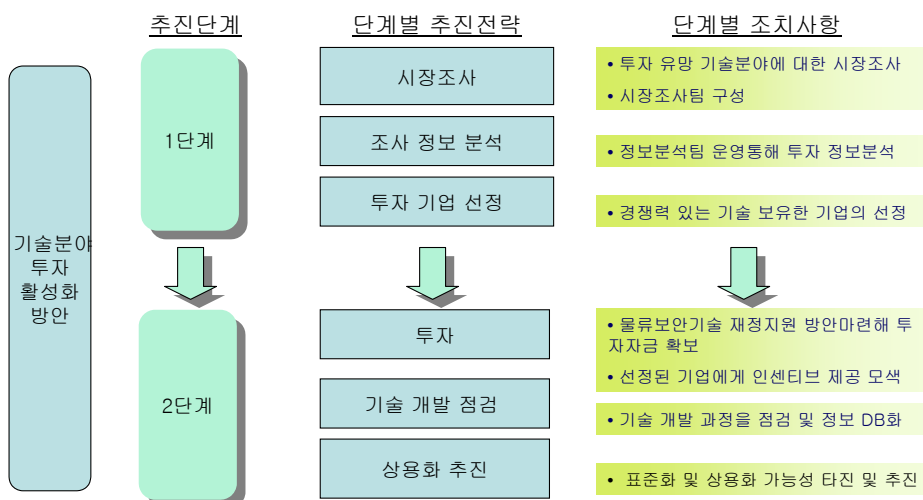
따라서 기술표준 부분에서의 이니셔티브를 확보하기 위해서는 우선 국제표준 가능성이 있는 분야를 선별하고, 이러한 분야에 대해 산업자원부 기술표준원을 중심으로 민간기업과 정부가 공동으로 논의하는 협력창구마련이 선행되어야 할 것이다. 이를 바탕으로 ISO를 중심으로 한 표준제정 작업에 적극적으로 참여하여야 할 것이다.

라. 기술부분 투자 활성화 방안 마련

위에서 언급한 기술연구 및 개발(R&D)은 정부의 적극적 지원과 민간기업의 전략적 투자를 바탕으로 한다. 이를 위해 단계별로 시장조사 및 조사정보 분석을 통해 경쟁력 있는 기술을 보유한 기업 선정이 우선 필요하다. 그리고 물류보안기술 재정지원 방안을 마련해 확보한 투자자금으로 기업에 투자하고 인센티브를 제공하는 방안도 함께 고려할 수 있다. 또한 계속적으로 기술개발과정을 점검하고 이 과정에서의 정보를 데이터베이스화해 이를 토대로 개발된 기술을 표준화 및 상용화할 수 있는 방안을 추진할 수 있다.

<그림 4-6>

기술부분 투자 활성화 방안



자료 : 한국해양수산개발원

2) 물류보안 전문인력의 육성방안

(1) 보안인증제도와 전문인력

물류보안은 생산자에서부터 최종소비자까지 공급망 전체에서 각각의 운송모드별로 보안이 확보되어야 한다(<그림 1-1> 참조).

공급망 전체 즉, 제조업자, 창고보관업자, 운송업자 및 서비스업자등 공급망에 연계되는 모든 조직에 대한 보안확보는 각각의 단계에서 보안을 확보하고 있어야 가능하다. 보안인증제도는 공급망에 있는 조직이 물류보안을 확보하고 있다는 것을 확인하고 인정하기 위한 제도이다. 보안인증을 받기 위해서는 먼저 각 업자나 업체 등이 보안위험성 평가를 기초로 보안경영시스템을 수립하고, 인증전문기관에서는 그 업체나 업자가 수립한 보안경영시스템에 관한 문서 또는 현장에 대한 심사를 해서 물류보안 확보를 위하여 요구하는 요건을 충족하고 있는 경우에 인증서를 교부하게 된다(<그림 2-1> 참조).

이러한 인증제도를 구축하기 위해서는 보안위험성 평가 전문가 및 인증심사전문가가 필요하다. 또한 각 업체등에서는 보안경영시스템의 유지 및 운영 책임을 담당하는 현장 전문가도 필요하다.

(2) 컨테이너 및 항만보안장치와 전문인력

보안인증을 받은 제조업자의 생산물은 대부분 컨테이너로 운송된다. 따라서 컨테이너 자체의 보안 확보가 물류보안의 중요한 부분이다. 컨테이너 자체의 보안은 생산지에서 화물을 적입하고 봉인한 후 최종 목적지에서 개봉될 때까지 봉인상태가 계속 유지되었다는 것을 확인하는 것이다. 컨테이너 보안에 사용되는 가장 기본적인 장치가 봉인이다. 그 동안의 컨테이너 봉인은 기계적 장치를 사용하여 왔는데, 운송과정에서 봉인장치가 훼손, 파손, 개봉되는 경우가 있었다. 컨테이너 봉인이 운송과정에서 훼손되는 경우는 단순히 화물의 도난 등으로 인한 손해 문제뿐만 아니라 보안측면에서도 문제가 있다. 특히 봉인된 컨테이너가 운송도중에 개봉된 후 다시 봉인되는 경우는 보안측면에서는 치명적인 문제가 되지만 현재의 봉인장치로는 그 확인이 쉽지 않다. 이로 인해 도입하고 있는 것이 컨테이너 전자봉인장치(e-Seal)이다. 컨테이너 내부에 장착하게 될 전자 보안장치는 화물의 도난, 파손, 복제로부터 보호하게 되며, 불법침입도 원격으로 확인할 수 있다. 불법침입을 확인하기 위해서는 인공위성 등을 통한 데이터 전송이 이루어져야 하며, 전송되는

데이터 등은 암호화되어 있어야 한다. 따라서 컨테이너 보안장치 및 데이터의 암호화 등 정보기술 분야의 전문인력이 필요하다.

생산지 또는 항만이나 공항의 보세장치장에서 화물을 적입하고 봉인한 컨테이너는 선박이나 항공기로 운송된다. 선박이나 항공기로 컨테이너가 운송될 경우 선박이나 항공기의 안전을 위하여 선적 전에 적재한 화물에 위험물이 없는지를 확인할 필요가 있다. 이러한 확인은 주로 항만이나 공항에서 이루어진다. 미국은 '9/11 테러대책 위원회의 권고를 이행하는 2007년 법률'로 미국으로 반입되는 모든 컨테이너 화물에 대한 100% 사전 검색을 의무화하였다. 이에 따라 미국으로 화물을 수출하는 항만은 향후 5년 이내에 컨테이너 화물 검색을 위한 관련 시설을 갖추고 사전검색을 의무화해야 한다. 공항이나 항만에서의 컨테이너 검색은 컨테이너를 적재한 차량이 항만이나 공항의 게이트를 통과할 때 이루어진다. 화물 검색 방법은 화물이 선적되기 전에 비파괴 영상장비와 방사능 탐지기를 사용한 2가지 검사, 즉 내장화물의 이미지 검색과 방사능 물질 탐재 여부를 검사하는 것이다. 따라서 컨테이너 검색기 등의 설치, 검색 및 검색기로 스캔한 내용의 판독 등 컨테이너 검색관련 보안장비의 설치 및 운영관련 전문가가 필요하다.

(3) 긴급계획과 전문인력

공급망 보안확보를 위해서는 보안 사고나 사건의 영향을 최소화하기 위한 위기 관리 및 복원 절차가 필요하다. 긴급계획의 경우 통상 보안평가를 거쳐서 보안계획을 수립하게 된다. 보안평가 수행자는 보안을 평가하는 적절한 기술을 보유한 전문가이어야 한다. 보안평가 결과를 토대로 수립하는 보안계획서도 일반인이 수립하기에는 어려운 점이 많아 통상 대행기관에 위탁하게 된다. 보안평가와 보안계획 수립에는 전문적인 지식이 요구되므로 전문가 양성이 필요하다. 또한 업체나 운송회사는 자체적으로 보안사고에 대비한 긴급계획 수립이 필요하다. 이러한 긴급계획을 유지할 책임이 있는 보안책임자 및 보안요원의 전문성 제고를 위해서는 교육이 필요하며, 이들을 교육시키기 위한 교육전문가 양성도 필요하다. 보안전문가를 현재의 학교교육체계에서 양성하는 것은 어려움이 있다. 정보시스템 분야 교육과정에는 보안과목을 추가하여 교육하여야 하며, 교육프로그램 개발도 신속히 이루어져야 한다. 가장 신속히 전문인력을 양성하는 방안은 무역업계 등 산업계에서 전문교육과정을 개설하는 것이다.

3. 물류보안 위기관리 및 복구 대책

1) 필요성과 외국의 사례

보안 사고나 사건의 영향을 최소화하기 위해서는 위기 관리 및 복원 절차가 마련되어야 한다. 위기관리 및 복원과 관련하여 참고할 수 있는 것이 2007년 5월에 싱가포르 세관이 도입한 ‘싱가포르의 안전한 교육 프로그램(STP)’이다. STP 가이드라인에 따르면 공급관련 업체들은 자신들의 업무처리와 공급 체인의 보안성을 증진시키기 위하여 일정한 요건을 충족해야 STP 업체로 인증받을 수 있다. 그 요건은 다음과 같다.

- i) 보안 관리 시스템을 갖추어야 한다.
- ii) 자신들의 작업수행에 대한 위험 평가를 실시해야 한다.
- iii) STP 가이드라인에 따라 보안조치를 취하여 유통라인의 보안을 확보해야 한다.

STP 가이드라인이 요구하는 보안 조치는 다음과 같이 8가지 요소로 구성되어 있으며, 위기관리와 사고수습도 하나의 요소로 포함되어 있다.

- i) 시설 보안과 접근 통제
- ii) 인력 보안
- iii) 사업 파트너 보안
- iv) 화물 보안
- v) 운송기관 보안
- vi) 정보와 정보 기술 보안
- vii) 사고 관리와 조사
- viii) 위기 관리와 사고 수습

위기관리를 위한 대책으로는 사고 또는 긴급 보안 상황에 대처하기 위한 긴급 계획(contingency or emergency plans) 수립을 요구하고, 사고수습을 위해 사업 지속 계획(BCP : Business Continuity Plan) 수립을 권장하고 있다. 긴급계획은 모든 고용인들에게 전달되어야 하며, 긴급계획에 의한 훈련을 주기적으로 실시해야 한다. 또한 운영 및 조직상의 변화에 맞춰 주기적으로 업데이트되어야 한다. 사업지속계획은 업체들에게 공급 체인에 영향을 주는 위기 및 사고당시, 그리고 사고 이후에

도 핵심 사업 기능(Critical Business Functions-CBF)이 유지될 수 있도록 수립할 것을 권장하고 있다.

국가 물류보안 기본계획을 수립하는 경우에는 그 내용에 STP 가이드라인에서 제시하는 바와 같이 긴급계획과 사업지속계획이 포함될 필요가 있다.

2) APEC의 물류보안 사고 사후 대응 체계

(1) APEC 대응계획

가. 개요

아시아태평양 경제협력위원회(APEC)는 2006년 고위급 회담(SOM : Senior Officer's Meeting)에서 APEC 물류보안(Total Supply Chain Security) 체계 구축의 일환으로 조속한 무역재개를 위한 프로그램(TRP : Trade Recovery Programme) 마련을 위한 연구그룹을 발족시켰다. 동 연구그룹에서 마련한 'APEC 무역재개프로그램'은 테러 공격 '발생 후' 경제적 파급효과의 최소화를 위한 APEC 차원의 대응체계 구축에 초점을 맞춘 것으로서 그 의미가 있다.

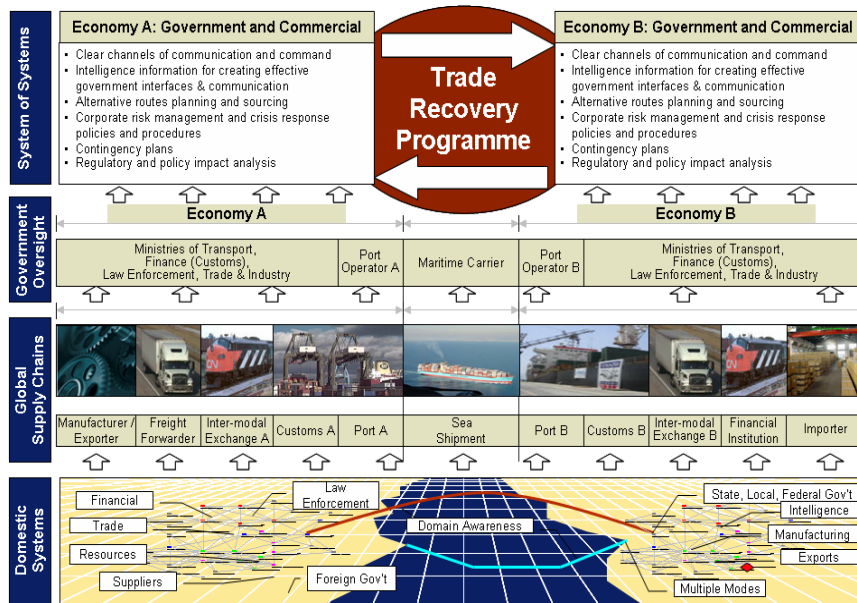
나. TRP의 내용

① 개념

TRP는 테러가 발생된 이후 신속한 무역재개를 확보하기 위해 필요한 주요 원칙, 범위 및 조건들을 제시하는 것을 의미한다. 이 개념에서 강조되는 사항은 국가 간 무역재개 활동들을 조정하며, 늦장대처로 인한 손실을 최소화하여 물류보안을 확립하는 것이다.

<그림 4-7>

TRP 개념도



② TRP의 내용

TRP는 i) 테러사건 발생 직후의 행동계획(Plan of Action), ii) 대응 모범 지침(model guideline), iii) 회원국간 의사소통(communication)의 3가지 요소를 주요 내용으로 한다. 행동계획은 APEC 회원국이 테러발생 후 신속한 무역재개를 위해 취해야 할 조치들을 차례대로 제시하고 있다. 모범 지침은 컨테이너 화물의 관리, 보안관리 및 사고 관리의 3가지가 핵심이다. 마지막으로 의사소통은 재개된 활동을 조정하기 위한 국가 간 네트워크에 대한 지침을 제공한다.

동 TRP는 WCO Framework, ISPS 및 ISO 28000 시리즈 등 물류보안에 대한 국제 규범을 수용하고 있다. 하지만 이들 규범을 대체하기보다는 물류보안의 사전적, 사후적인 확보를 위해 이들 규범을 보완하고 있으며, 나아가 각국의 국내공급망 프로그램을 지원하는 역할을 수행한다. 또한 TRP는 확정된 것이 아니며 이후 각국의 필요에 의해 수정, 보완된다.

다. 테러발생 직후의 행동계획

테러발생 직후의 행동계획(Plan of Action)은 TRP를 가동하기에 충분한 테러행위가 발생한 경우 즉각 준수해야 하는 행동들을 순차적으로 제시한 것이다. 이 계

획의 목적은 화물을 고 위험·저 위험 군으로 효율적으로 분리하기 위한 것이다. 테러 발생 후 취하여야 할 행동들을 순차적으로 제시하기 위해서 무역을 단절시키는 경우를 시나리오로 제시하였다.

수많은 잠재적 테러공격 시나리오가 있지만, 제시된 시나리오는 잠재적 테러공격 대응을 위한 유용한 정보를 제공할 것이다. 이 시나리오에 따라 시나리오 순차도(Process Map)도 제시하였는데, 테러가 발생한 국가에서 수행하여야 할 일련의 행위들을 시각적으로 제시하고, TRP에 참가하고 있는 모든 국가들이 수행하여야 할 행위도 나타내었다.

<표 4-5>

시나리오의 내용

시나리오	두 개 이상의 CBR 장치가 컨테이너에 선적되어 복수의 APEC 회원국의 항만에 도착한다. 그 장치들이 작동하였고, 다른 회원국에도 이러한 장치들이 있을지 모르는 상황으로 알려져 있다. 사건이 발생한 항만 터미널에 공격으로 인한 오염(Contamination)이 발생하였는지는 모르는 상황이다. 양쪽 항만 인프라에 피해가 발생하였다.
위협벡터(Vector)	독립된 선박에 CBR 장치가 설치되었다. 선박은 동일한 또는 다른 외국항만으로부터 온 것이다.
공격지점	회원국 A, 항만 A, 민간터미널 A 회원국 B, 항만 B, 민간터미널 B
대응(Reaction)	• 테러발생국은 TRP 절차를 가동한다. • 회원국들은 항만폐쇄, 접근 통제 및 항만근접 항해선박의 우회 등을 결정할 수 있다. • 테러발생 항만 또는 그 인근지역으로의 접근은 긴급대응팀과 주요 항만 관리인력으로 한정된다. • 테러에 노출된 화물과 인력의 오염제거작업(decontamination) • APEC국가는 모든 수입품에 대한 검색 및 스캔작업을 실시할 수 있다. • 사고발생 후 항만 인프라 시설에 대한 수리 및 오염제거작업. • 승객명단 및 적하목록에 대한 추가적 정보가 고려될 수 있다. • 테러가 발생하지 않은 국가의 항만운영이 검토되고 필요하다면 일시적으로 제한될 수 있다. 즉 무역흐름이 일시적으로 영향을 받을 수 있다. • APEC 회원국들은 필요한 보안 및 검색조치와 위협평가를 위한 일상적인 위험분석표에 대해 동의함. • 저위험화물을 우선적으로 처리함과 더불어 고위험 화물을 저위험 화물과 분리시킨다.

<표 4-6>는 무역을 단절시키는 주요한 사건이 발생한 경우를 가정하여 제시된 기본적인 시나리오를 내용으로 한 APEC 국가에서 발생한 생화학 및 방사능공격(CBR)이 항만에 발생한 경우 추가적인 공격의 위험을 가정하여 수립된 것이다.

APEC의 대응모범지침에 따라 이러한 테러발생 직후의 행동계획도 수립하여야 한다.

<표 4-6>

시나리오의 순차도⁷⁶⁾

Activity Flow →

	대응(Respond)		복구(Repair)		재건(Reconstitute)	무역재개(Resume)	검토(Review)
사건 발생국 (Event Economies)	TRP의 실시 요구 (Request Initiation of TRP)		행동 피해 평가 (Conduct Damage Assessment)		인프라의 재건 Restore Infra Structure	영향을 받은 항만의 운영/능력의 향상 Increase Operations/Capacity of Affected Port(s)	행동과 결과의 검토 Review Actions & Results
	공격양태화정 Characterize Attack Type/Vectors	영향받은 컨테이너 식별 Identify Affected Containers	보안 갭/취약성 식별 Identify Security Gaps/Vulnerabilities	컨테이너 스크린/스캔 Screen/Scan Containers	컨테이너 프로세스 Process Containers	노선 변화 Establish Route Changes	
		영향받은 컨테이너 분리 Isolate Affected Containers	새로운 스크린/스캔방법에 대한 협력 Collaborate on New Screening/Scanning Measures		새로운 스크린/스캔방법의 이행 Implement New Screening/Scanning Measures		
	항만운영에 대한 영향결정 Determine Impact on Port Operations		합동 조사의 실시 Commence Joint Investigation				
	잠재적 위험식별 Identify Potential Risks	임시보안조치의 이행 Implement Interim Security Measures	인프라시설 및 화물에 대한 오염제거작업 Decontaminate Infrastructure and Cargo		오염된 컨테이너의 가공 Process Contaminated Containers		
	TRP파트너와 연합 의사소통의 설립 및 유지 Establish and Maintain Joint-Communication with Partners						
공유된 행동 (Shared Activities)	TRP 실시 Initiate TRP		새로운 안보조치에 대한 협력 Collaborate on New Security Measures		업데이트된 조치의 이행 Implement Updated Security Measures		업데이트된 TRP 실천계획 Update TRP of Action
	긴급대응실행/무역 상황계획 Execute Emergency Response/Trade Contingency Plans		● 새로운 운영절차에 대한 협력 Collaborate on New Operating Procedures		● 새로운 운영절차의 이행 Implement New Operating Procedures		
다른 회원국 (Economies)	사건 발생 국가로부터 업데이트된 자료받기 Receive Updates from Event Economies						행동과 결과의 검토 Review Actions & Results

76) 시나리오 순차도는 구별을 위해 파랑색은 컨테이너/화물 관리, 녹색은 보안관리, 회색은 사고관리 및 적색은 필요한 커뮤니케이션을 나타내고 있음.

3) 물류보안 사고 대비 국가긴급계획⁷⁷⁾

(1) 긴급계획 수립시 고려사항

가. 계획 수립 및 책임기관 지정

물류보안사고 대비 국가긴급계획 수립에 앞서 국가 및 지역차원에서 긴급계획 업무를 책임지는 기관을 지정해야 한다. 국가긴급계획은 통상적으로 고도의 조직 관리 차원에서 개발되는 반면에, 지역긴급계획은 사고발생시에 현장대응노력들의 조정을 책임지는 지역기관에 의해 개발된다.

여러 기관 또는 조직이 물류보안과 관련하여 다양한 기능들을 분담하고 있지만, 긴급계획의 성공적 운영을 위해서는 지정기관이나 주도기관이 동 계획을 총괄 조정해야 한다.

나. 대응조직

국가긴급계획의 수립 이전에 국가대비·대응체계가 구축되어야 한다. 국가체계는 여러 수준의 대응체계로 구성할 수 있지만 적어도 국가차원의 긴급계획 및 지방차원의 긴급계획은 수립되어야 한다. 지방차원의 계획은 항만이나 공항을 중심으로 한 특정지역 또는 지방자치단체를 단위로 수립될 수 있다. 지방긴급계획의 범위내의 항만이나 공항은 각각의 단위별로 긴급계획을 수립하여야 한다.

대응조직은 일정한 규모와 특성의 오염사고를 처리할 수 있을 정도로 충분히 커야 하고, 보다 광범위한 작업을 수행하기 위하여 확장 및 개편이 가능한 유연성 있는 조직이어야 한다.

실질적인 보안사고 및 보안사고 우려에 관한 정보의 신속한 수집 및 전달을 위한 체계가 구축되어야 하고, 대응조직의 의사결정자가 언제든지 이러한 정보를 접수하여 이용할 수 있게 지시와 정보의 전달을 위한 적절한 통신시설이 준비되어야 한다.

대응조직의 의사결정자는 보안사고에 신속히 대처하기 위한 조치를 취할 수 있

77) 국제해사기구(IMO) 해양환경보전위원회(Marine Environment Protection Committee)는 선박이나 해양 시설에서의 기름오염을 대비한 긴급계획에 관한 지침서(Section II, Manual on Oil Pollution, Contingency Planning)를 발간하였다¹⁾. 이 지침서는 물류보안을 위한 긴급계획 수립 지침은 아니지만 국가긴급계획 수립시 고려사항 및 긴급계획에 포함될 내용 등은 국가물류보안 긴급계획 수립에도 적용할 수 있다. 이하에서는 이 지침서를 토대로 물류보안 긴급계획 수립시 필요한 사항 및 긴급계획 수립시 포함되어야 할 내용을 제시한 것이다.

는 충분한 권한을 부여받아야 한다. 대응조직에는 관련기관의 활동을 조정하고 다수의 보안인력 및 다양한 장비를 통제할 수 있는 권한이 주어져야 한다. 따라서 대응조직의 부서별 책임을 명확히 하는 지침이 필요하다.

다. 업체와의 협력

효과적인 대응체계의 구축과 유지를 위하여 업체와의 협력이 중요하다. 정부의 역할은 이러한 협력관계를 위한 법적·조직적 체계를 구축함으로써 정부와 업계의 역할을 명확히 해야 한다.

미국의 C-T PAT 참여업체, 유럽연합의 인증받은 운영자(Secure Operator Scheme), 싱가포르의 물류보안파트너쉽제도(STP), 그리고 세계관세기구(WCO) SAFE Framework의 승인된 운영자(Authorized Economic Operator) 등 민관협력프로그램에서 알 수 있듯이 물류보안 확보를 위해서는 업체와의 협력이 필수적이다.

라. 단계별 대응

단계별 대응은 대응수준을 편리하게 구분하고 계획수립에 필요한 실질적 기초를 제공하기 위하여 대응계획 수립에 필요한 개념이다. 통상 1단계는 항만이나 공항 단위에서 처리할 수 있는 규모이며, 2단계는 항만이나 공항이 소속된 지방자치단체 차원에서 처리할 수 있는 규모이다. 2단계에서는 인접 지방자치단체의 지원을 요구할 수 있다. 보안사고의 규모에 따라 대응시나리오를 준비한다. 3단계는 이용가능한 모든 국가자원을 동원해야 하는 보안사고의 경우이다. 상황에 따라서는 지역적·국제적 시스템까지 동원할 수 있다.

마. 보안사고 고위험지역의 명시

보안사고에 대한 대응능력을 결정하기 위해서는 위험이 높은 지역을 명확하게 파악하는 것이 중요하다. 또한 우선적으로 보호해야 할 지역이나 시설을 결정할 필요가 있으며, 이러한 의사결정 전에 이해당사자와 협의를 거쳐야 한다.

협의를 우선순위에 관한 정보는 일반인이 쉽게 이용할 수 있도록 우선순위의 목록을 작성하여 배포하여야 한다. 이러한 우선순위의 목록작성은 보안사고시 곤란한 문제에 직면한 경우의 의견 불일치 및 의사결정 지연 등의 위험을 감소시킨다.

(2) 물류보안사고 대비·대응을 위한 국가체제

가. 목적 및 목표

물류보안사고 대비 국가긴급계획은 화물의 제조에서 최종소비에 이르는 과정에서 발생한 보안사고에 대응하기 위해 공적·사적 자원을 포함하는 범국가적 긴급대비 및 대응체제를 마련하는 것이다.

이러한 계획은 보안사고 위험이나 보안사고에 대해 적시에 효과적인 대응을 보장하는 것을 목표로 하고 있다. 그 목표를 달성하기 위해 필요한 조치는 다음과 같다.

- i) 모든 관계기관이 포함된 실행 가능한 운영조직의 구축
- ii) 고위험지역 및 보호우선순위 설정
- iii) 보호지역을 보호하기 위해 사전 배치되는 대응장비의 최소 수준 및 적절한 형태 유지
- iv) 운영요원, 중간 및 상급관리요원의 훈련 실시
- v) 연습을 통한 평가 및 개선

나. 계획의 범위 및 내용

대부분의 보안사고는 지역차원에서 처리될 수 있지만, 대형 보안사고의 경우는 국가적 및 국제적 수준까지 단계적으로 확대하여 대응할 수 있어야 한다.

긴급계획에 보안사고에 대한 정책과 책임을 명시하고, 관계법령의 제·개정을 비롯하여 긴급계획의 준비와 이행을 책임지는 당국 또는 대표기관을 지정해야 한다. 근거법령에는 긴급계획의 지리적 관할범위가 명시되어야 한다.

다. 관련기관으로부터의 지원

긴급계획의 수립 및 실행단계에서 현장책임자에게 장비나 인력 등 자원이나 기술적·과학적 조언을 제공할 수 있는 관련 정부기관과 민간기관의 업무를 긴급계획에 명시해야 한다. 관련기관의 지원에 있어서 고려되어야 할 항목은 다음과 같다.

- i) 보안사고 대응조직을 원조하기 위한 지원관들의 공동작업 방법
- ii) 지원그룹이 수행할 수 있는 조언, 평가책임 및 기술업무의 형태
- iii) 지원기관의 작업을 대응담당관에게 전달할 수 있는 조직적 연계수단
- iv) 논쟁 또는 상충하는 의견을 해결하는 기구에 대한 필요성

라. 보고체계

물류보안사고 또는 사고 우려에 대한 정보는 다수의 출처로부터 나올 수 있다. 긴급계획에는 사고관련정보를 접수·전파할 기관을 지정해야 한다.

마. 경보체계

초기보고 및 후속보고를 가능한 한 신속하게 보안책임기관과 지원기관에 전파하기 위한 정보절차가 긴급계획에 포함되어야 한다.

바. 보안사고 평가

물류보안사고로 생긴 위험에 대한 신속한 평가는 필수적이다. 실제보안사고가 발생한 경우, 그 물류운송시스템에 미치는 영향과 잠재적인 위협을 점검하기 위한 손해평가가 지속적으로 이루어져야 한다.

사. 대응결정

긴급계획에서는 다음의 사항을 고려하여 다양한 대응선택들을 마련해야 한다.

- i) 가능하면 보안사고로부터 피해 최소화
- ii) 우선보호순위를 고려하여 시나리오에 따른 신속한 대응작업 수행
- iii) 필요한 방제요원, 장비, 기자재 이동

아. 연락체계

긴급계획에는 현장책임자·현장과 보안사고가 발생한 시설간에 효과적인 통신을 위한 체계 및 절차를 마련되어야 한다. 통신센터는 최소한 전화, 팩시밀리, 텔렉스 및 라디오의 통신장비를 갖추고, 무선통신을 위한 사용주파수가 할당되어야 한다.

자. 훈련 및 연습

훈련 및 연습에 관한 요건이 긴급계획에 명시되어야 한다. 대응 장비 운전자, 현장책임자, 지원요원 등을 포함하는 모든 수준에서의 훈련프로그램이 개발되어야 한다.

긴급계획의 실효성을 평가하기 위하여 긴급계획 주관기관이 자체 요원 및 자원에만 관련하여 내부 방제연습을 실시한다. 상이한 긴급계획들의 연계성을 점검하기 위해 외부 대응훈련이 필요하다. 외부대응 훈련은 긴급계획 주관기관의 대응구조 외에도 정부나 업체에 제공되는 요원 및 자원이 포함되기 때문이다.

대응요원·장비·자재의 유효성과 수행능력을 확인하기 위한 이들의 기동성

및 실제적인 투입이 요구되는 대응훈련을 수시로 실시하여야 한다.

차. 긴급계획의 개정

긴급계획은 정기적인 훈련이나 실제 보안사고로부터 얻어진 경험을 반영시키기 위해 주기적으로 재검토되어야 하고, 긴급연락망과 장비목록의 정기적인 갱신이 필요하다. 대응조직이나 정책에 영향을 미치는 조직상·법률상의 변화는 관련 긴급계획을 적시에 변경하여 반영되어야 한다.

제5장 물류보안산업 전망 및 육성방안

1. 물류보안산업 동향 및 규모

1) 물류보안산업의 최근 동향

(1) 물류보안산업의 급성장

2001년 9·11 테러는 역설적이기는 하지만, 새로운 비즈니스 모델을 개발하는 계기가 되었다. 각국이 물류보안조치를 강화하고, 이에 소요되는 인적·물적 시스템을 개발하면서 하나의 거대한 ‘물류보안산업 내지는 시장’이 형성되기 시작한 것이다. OECD가 2003년에 예측한 자료에 따르면, 당시 국제해사기구(IMO)가 도입한 ISPS 코드를 이행하는데 따른 전체 비용이 초기 투자비용으로 40억 달러, 그리고 연간 유지비용으로 10억 달러 이상이 들어가는 것으로 추정되었다.

앞으로도 물류보안시장의 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 제도인 데 비해 미국과 세계관세기구(WCO) 등에서 마련한 제도는 물류 전 구간을 대상으로 하는 특징이 있다. 물류보안이 확대됨에 따라 그 비용도 크게 증가할 것이 분명하다.

물류보안시장에 참여하고 있는 글로벌 기업의 추산에 따르면, 컨테이너 보안 장비(CSD) 및 컨테이너 검사장비, 전자 태그(RFID) 및 스마트 컨테이너 등 물류보안시장의 규모는 2010년에 연간 90억 달러에 달할 것으로 예상되고 있다. 국제표준화기구(ISO)가 보안표준의 제정을 추진하고 있는 것과 별도로 미국의 록히드 마틴 그룹과 GE가 포함된 국제컨테이너보안협회(ICSO)⁷⁸⁾가 각각 보안기술과 장비에 대한 개발사업을 진행하면서 물류보안 시장을 장악하기 위해 치열하게 경쟁하고 있는 이유도 바로 여기에 있다.⁷⁹⁾

78) International Container Security Organization의 약자임.

79) 삼성물산은 2006년에 150억 원을 투입, GE의 자회사인 컴머스가드(Commercegaurd)의 아시아 판매권을 확보하였으며, 해양수산부는 전자 태그(RFID) 테스트, 설치 및 실제 항만에서 적용하기 위한 데이터 처리 등에 대한 시범(표준화) 사업을 추진하고 있음.

(2) 글로벌기업의 물류보안시장 참여

이 같은 움직임과 관련해 최근 두 가지 중요한 변화가 나타나고 있다. 이른바 스마트 컨테이너 관련 기술의 개발과 보급을 주도해온 사비 테크놀로지(Savi Technology)⁸⁰⁾가 대형 군수업체인 록히드 마틴에 인수되었다는 점과 국제컨테이너보안협회(ICSO)가 창설되어 물류보안에 관한 국제 표준과 기술 개발에 적극 나서고 있다는 점이다.

사비 사는 전자 태그(RFID)에 기반을 둔 화물 추적 시스템을 개발해 운영하고 있는데, 현재 미국 국방부와 북대서양조약기구(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 태그와 신호 판독기, 중앙 데이터베이스에 화물 정보를 올릴 수 있는 무선 네트워크 시스템, 그리고 컨테이너 상태를 전송소프트웨어를 개발해 고객에게 제공하고 있다.⁸¹⁾

이 같은 사비 사가 록히드 마틴에 인수됨에 따라 미국에서 이와 유사한 시스템을 개발·기술 승인을 목표로 두고 있는 제너럴 일렉트릭(GE)사가 개발한 ‘컴머스가드(CommerceGuard)’와의 경쟁이 더욱 치열해질 전망이다.

특히 국제컨테이너보안협회의 창설로 사비와 GE와의 보안 시스템 개발 및 판매, 국제 표준 경쟁은 더욱 가열될 가능성이 커졌다. 사업자 단체인 이 기구는 앞으로 주로 컨테이너 보안장비와 관련된 시스템을 개발하고 국제 표준을 발표하는 것을 설립 목적으로 설정하고 있다. 공교롭게도 이 기구의 창설 회원으로 참여하고 있는 업체들이 사비 사와는 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. 우리나라 삼성물산도 2006년에 1,500만 달러를 투입, 이 사업에 참여하고 있다.

(3) 글로벌 물류보안 솔루션

현재 시행되고 있거나 향후 도입이 예정되어 있는 물류보안제도와 관련하여 필

80) 사비 사는 HPH와 싱가포르 투자회사인 테마섹 홀딩스, NOL, APL 및 싱가포르에어라인, MOL, 오라클 등 세계 굴지의 물류 회사와 솔루션 업체 등이 투자해 캘리포니아 서니베일에 설립한 민간 기업임.

81) 2005년에 사비 사와 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. 이 회사가 전자 태그를 기반으로 개발한 컨테이너 화물 물류보안 솔루션의 상품명은 ‘사비 트랙(SaviTrak)’임.

요한 시설 및 장비, 그리고 정보통신산업(IT)에 기반을 둔 보안 솔루션 분야는 무궁무진하다는 평가다. 주로 컨테이너 화물에 들어있는 위험화물을 가려내는 장비와 제조업체 또는 항만 터미널 등 물류 핵심시설에 대한 비인가자 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 샌디에이고에 본부를 둔 SAIC와 스미스 디텍션(Smith Detection)사가 양분하고 있는 실정이다.

전자의 경우 ICIS⁸²⁾라는 토털 솔루션으로 방사능 물질 탑재 여부까지 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 검사하는데 X-레이 기술을 이용할지 또는 감마 레이 기술을 이용할지 여부와 검사 정보를 화물 정보와 통합, 관리하는 최적의 정보관리 시스템을 개발하는 것 등이다.

또한 비인가자 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 있다. 미국의 경우 최근 근로자 등에 대한 신원 조사와 새로운 신분증 발급 제도를 도입했다. 인접국인 캐나다도 이에 따르고 있다. 앞으로는 지문과 손금, 홍채 및 얼굴 등이 카드에 삽입되는 이른바 생체 인식 기술 스마트카드 및 판독기(리더기)가 일체를 이룬 출입 통제 장비가 도입될 것으로 보인다. 이 시장의 규모는 미국을 기준으로 향후 10년 동안 10억 달러 이상으로 추정되고 있다. 민간 기업뿐만 아니라 정부에서 물류보안산업을 차세대 성장 동력으로 적극 육성해야 하는 이유가 여기에 있다.

(4) 컨테이너 전자봉인 표준 결정

물류보안 솔루션과 관련해 최근 매우 중요한 합의가 도출되었다. 국제표준화기구(ISO)가 컨테이너의 전자 잠금장치에 대한 국제표준 규격을 확정하였다. 국제표준화 기구는 2007년 5월 10일 우리나라 부산에서 정부 대표자들이 참석한 가운데 기술위원회(TC 104) 회의를 개최하고, 컨테이너 전자 봉인 장치(E-seal)에 대한 국제 표준을 채택하였다.

82) Integrated Container Inspection System의 약자임.

<표 5-1>

전자 봉인관련 표준 문서

문서번호	주요 내용
ISO 18185-1	Communication Protocol (통신 프로토콜)
ISO 18185-2	Application Requirements (응용 요구사항)
ISO 18185-3	Environmental Characteristics (동작 환경특성)
ISO 18185-4	Data Protection (데이터 보호)
ISO 18185-5	Physical layer (물리계층 특성)

자료 : 한국해양수산개발원

ISO는 이번 회의에서 컨테이너 잠금 장치에 사용되는 전자 태그(RFID)의 주파수를 433Mhz와 2.45Ghz 모두 지원하는 이른바 ‘듀얼 밴드’로 확정했다. 다만, 전자 봉인 장치 리더기는 433Mhz와 2.45Ghz 중 하나를 지원하면 된다.

이에 따라 앞으로 업계에서 컨테이너 전자 봉인 장치를 개발할 때는 이 기준에 따라야 하고, 정부 또한 이 기준에 맞는 봉인장치를 승인하는 절차를 마련해야 한다.

컨테이너 전자 봉인 장치는 9·11 테러 이후 테러리스트들이 컨테이너를 무단으로 개폐하는 것을 막는 최첨단 장치로, 그 동안 글로벌 기업들이 시장을 장악하기 위해 치열하게 경쟁해왔다. 현재 컨테이너 봉인장치 시장은 433Mhz에 기반을 둔 미국의 록히드 마틴 그룹(Savi Networks)과 2.45Ghz의 제너럴 일렉트릭(GE) 그룹이 양분하고 있는 상태이다.⁸³⁾

전문가들은 이번 회의에서 컨테이너 전자 봉인 장치가 예상을 뒤엎고 듀얼 밴드로 결정된 것은 원천기술을 갖고 있는 미국 기업의 승리로 풀이하고 있다. 이에 따라 앞으로 업계에서 컨테이너 전자 봉인 장치를 개발할 때는 두 회사에 특허 사용료(이른바 로열티)를 내야 하는 부담을 안게 됐다. 특히 사비 네트워크스는 이번 에 채택된 문서에 자신이 개발한 기술을 사용할 때는 사전 승인을 받아야 한다는 강제조항을 넣는 데 성공함으로써 앞으로 엄청난 로열티를 받을 수 있을 것으로 전문가들은 전망하고 있다.

한편, 듀얼 밴드가 표준이 됨에 따라 선사 또는 화주 입장에서는 433Mhz와 2.45Ghz를 모두 지원하는 컨테이너 전자 봉인장치를 구입해야 하므로 비용이 상승할 우려가 있다는 의견도 제기되고 있다. 그런데 이보다 더 큰 문제는 ISO 컨테이너 전자 봉인장치 표준이 미국의 항만보안법에 규정돼 있는 이른바 컨테이너

83) 우리나라의 삼성물산은 GE가 원천기술을 갖고 개발한 컨테이너 보안 장치(상품명 Commerce Guard)에 2006년에 1,500만 달러를 투자, 아시아 12개국의 판권을 갖고 있음.

보안 장치(CSD)와 크게 달라 향후 사용에 따른 혼란이 일어날 가능성도 있다는 점이다. 기본적으로 ISO의 컨테이너 전자 봉인장치는 컨테이너 뒤쪽 외부에 부착하도록 되어 있으나 미국의 CSD는 컨테이너 내부에 붙이는 것으로 되어 있고, 오작동 비율도 미국이 낮을 수 있기 때문이다.⁸⁴⁾

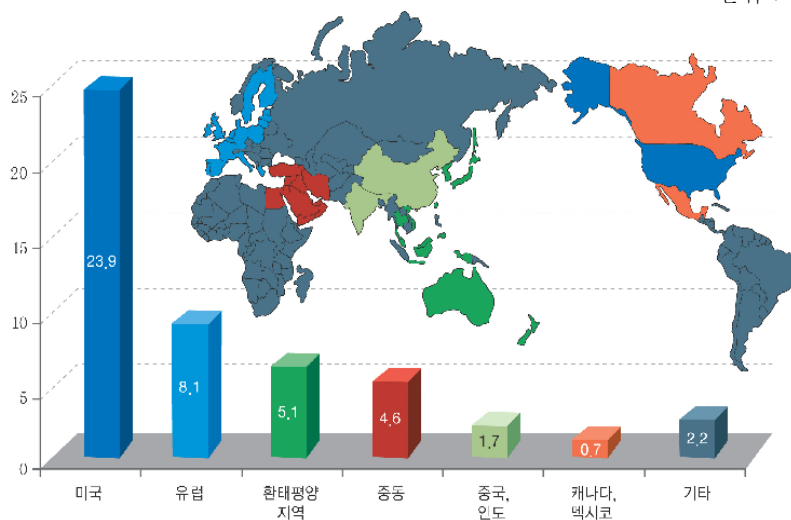
2) 글로벌 물류보안산업 규모⁸⁵⁾

전 세계적인 물류보안산업관련 시장 규모는 2005년 기준으로 약 464억 달러⁸⁶⁾ 정도로 추산되고 있다.

<그림 5-1>

세계 보안산업 시장규모(2005년)

단위 : 10억 달러



자료 : Home Land Security Research

지역별로 살펴보면, 미국 시장이 239억 달러로 세계시장의 약 52%를 차지하고 있으며, 유럽이 81억 달러, 호주를 포함한 일본, 한국 등 환태평양 지역이 51억 달러, 중동 지역이 46억 달러, 중국과 인도가 17억 달러, 캐나다 및 멕시코 지역이

84) 그러나 이 같은 우려에도 불구하고 일각에서는 ISO의 컨테이너 전자 봉인장치 표준을 결정할 때 미국이 회의를 주도하기 때문에 2007년 상반기에 발표되는 미국의 컨테이너 보안표준도 결국 ISO기준을 수용하는 방향에서 결정할 것이라는 의견이 나왔음(JOC, 2007년 6월 4일자).

85) 이 내용은 협동연구사업에 의해 집필된 것으로 인하대학교 민정웅 교수 및 이상윤 교수가 작성했음.

86) Home Land Security Research, 2005.

7억 달러이며, 나머지 지역이 22억 달러 정도로 추산되고 있다. 이 같은 시장 규모에서 한 가지 중요한 시사점은 아래의 표와 같이 향후 10년간의 예측된 시장 성장률에서 미국보다는 유럽, 인도 및 중국의 성장률이 훨씬 높다는 사실이다.⁸⁷⁾

<표 5-2> 2015년까지의 보안 분야 시장 성장률 전망

지 역	2005년도		2010년도		2015년도	
	억달러	%	억달러	%	억달러	%
중 동	46	10%	98	9%	152	9%
유 럽	81	17%	215	20%	396	22%
호주, 일본, 환태평양	51	11%	109	10%	163	9%
중국, 인도	17	4%	69	6%	168	9%
캐나다, 멕시코	07	2%	18	2%	33	2%
미 국	239	52%	497	47%	748	42%
기 타	22	5%	62	6%	124	7%
총 계	464	100%	1,068	100%	1,783	100%

자료 : Home Land Security Research

보다 구체적으로는 하드웨어 부문의 시장규모가 향후 폭발적인 성장세를 보일 것으로 예측된다. 단편적인 예로, 스마트 컨테이너 시장의 경우 2006년 약 7천만 달러 규모에서 2012년에는 2006년 대비 약 60배 정도인 42억 달러로 예측되고 있다.⁸⁸⁾ 이러한 시장의 급격한 팽창은 관련 산업, 특히 전자산업에도 긍정적인 영향을 미칠 것으로 분석되고 있다. Home Land Security Research의 자료(2005)에 의하면, 2001년 현재 항공보안 분야를 중심으로 약 10억 달러 정도에 그치고 있는 전자산업 내 보안관련 규모가 2005년에는 50억 달러 규모로, 그리고 2010년까지는 최대 200억 달러 규모로 2005년 대비 약 4배 정도 성장할 것으로 예측되었다. 이는 연평균 37% 이상의 급격한 성장세이다.

이러한 급격한 성장세는 지난 2001년 9·11 테러 이후 많은 보안전문가들이 기존의 보안에 사용되는 대부분의 전자기기에 대한 신속한 교체가 필요하다는 주장이 제기되면서 시작되었다. 실제로 과거 사용되던 기기들은 대부분 1990년대에 사용되었던 낙후된 장비가 대부분이기 때문에 이에 대한 대대적 교체가 필요하게 된 것이다. 또한 대량살상무기 통제와 같이 미국 정부를 중심으로 한 새로운 구상

87) Home Land Security Research, 2005.

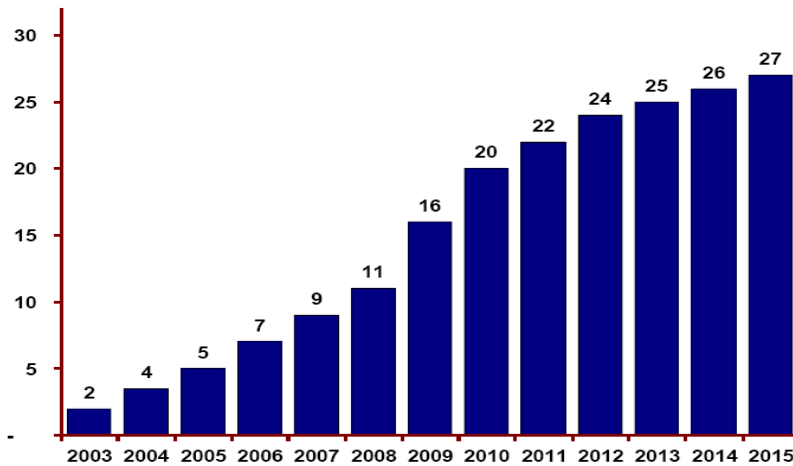
88) Home Land Security Research, 2005.

이 적극적으로 추진되면서 최첨단 기술을 활용한 센서, 감시 장비, 생화학 측정 장비들에 대한 수요가 새롭게 발생하게 되었다. 향후 시장에서 많은 수요를 가지게 될 장비의 분야로는 각종 무선감지장치(센서), 전파 관련 장비, 통신관련 기기 및 장비, 전자 태그(RFID), 폐쇄회로 감시 장비(CCTV), 생체감지기 등이다.

<그림 5-2>

전자산업 내 보안 분야의 시장 규모⁸⁹⁾

단위 : 1억 달러



자료 : Home Land Security Research.

이와 같은 물류보안 관련 시장 규모의 급속한 확대에 대응하여 최근 글로벌 업체를 중심으로 컨테이너 보안 장비, 시스템 및 솔루션 사업에 참여하는 기업도 증가하고 있다.

현재 전자 태그(RFID)를 핵심으로 하는 컨테이너 보안장비 시장은 미국의 GE 연합체와 군수업체인 록히드 마틴 그룹으로 양분되어 있다. 먼저, GE는 컨테이너 내부에 전자 태그를 부착, 운송되는 도중에 부정개폐가 이루어졌는지의 여부를 확인하는 자사 개발 물류보안 시스템인 CommerceGuard의 해외시장 선점을 적극적으로 추진하고 있는데, 우리나라의 경우 삼성물산이 1,500만 달러를 투입, CommerceGuard 지분 10%를 인수함으로써 아시아 12개국에 대한 판매권을 확보, 컨테이너 보안 시장에 진출한 바 있다. 이와 함께 록히드 마틴의 자회사인 사비(Savi)는 세계 최대의 글로벌 터미널 운영업체인 허치슨 포츠 홀딩스(Hutchison Ports Holdings)가

89) Home Land Security Research, 2005.

지분을 보유하고 있는 기업으로서 물류 요충지역에 분포되어 있는 허치슨 터미널을 중심으로 CommerceGuard와 유사한 시스템을 구축하여 왔다. 현재 사비의 컨테이너 보안장비 시스템은 미국의 버지니아 항만을 비롯하여 부산의 허치슨 터미널과 홍콩, 로테르담, 펠릭스토우 항만 등에 설치되어 있다.

컨테이너 물류보안 시장은 아직 초기단계로서 물류보안 장비 시장을 중심으로 발전하고 있으며, 향후 물류보안과 관련된 컨설팅, 교육, 금융, 보험 등 시장이 분화될 것으로 예상된다. 본 절에서는 먼저 현재 물류보안 시장의 대부분을 점유하고 있는 물류보안 장비 시장 규모에 대해 간단히 살펴보고자 한다.

(1) 화물 검색기/방사능 탐색기 시장

컨테이너 보안기준은 컨테이너가 국제적으로 운송되는 과정에서 부정한 방법으로 개폐되었는지의 여부를 확인하는 장비에 대한 표준을 의미한다. 2003년 HSRC(Human Sciences Research Council)의 예측에 따르면, 미국 컨테이너 검색기 시장의 규모는 2002년 7천만 달러에서 2010년 4억 4천만 달러로 650% 성장할 것으로 전망하였다. 이에 비해 2006년 Frost & Sullivan⁹⁰⁾은 미국 컨테이너 검색기 시장의 규모가 2006년 3억 8천만 달러에서 2013년에는 12억 7천만 달러로 증가세를 나타낼 것으로 예상하였다. 이와 같이 약 3년의 시차를 둔 양 기관의 시장 전망에 큰 차이가 있는 것은 컨테이너 검색기 시장이 정상적인 예측 범위보다 훨씬 급속하게 성장하고 있음을 반영하는 것으로 풀이된다.

한편, 방사능 탐색기의 시장규모와 관련하여 미국의 Instrument Business Outlook(2006)은 NII 시스템(non-invasive imaging system)을 제외한 방사능 탐색기의 전 세계 시장 규모가 2005년의 2억 6,200만 달러에서 2006년 3억 달러로 14.5% 성장하였고, 2007년에는 전년 대비 13.7% 증가할 것으로 추정하였다. 2005년 기준 북미지역의 방사능 탐색기 시장은 세계시장수요의 45%를 점유한 것으로 보고되었다.

(2) 컨테이너 전자 봉인장치 시장

E-Seal(Electronic Seal)이라 불리는 컨테이너 전자 봉인은 능동형 전자 태그(Radio Frequency Identification) 기술의 대표적인 응용으로서 화물 컨테이너의 문이 비정상적인 형태로 개폐됨을 감지하거나 또는 비정상적인 개폐 시도를 감지하여

90) Frost & Sullivan, Container Security - A Market Analysis, 2007. 3.

주변에 설치되어 있는 리더(reader)에게 알리고, 그 이력을 유지하는 역할을 한다. 전자봉인 시스템은 다음과 같이 물류 체인 전반에 걸쳐 이익이 될 것으로 기대되고 있다.

- 컨테이너 흐름을 용이하게 하며 게이트에서의 확인 시간을 감소시킨다.
- 컨테이너 이동과 인벤토리 추적을 가능하게 함으로써 효율성과 보안성을 향상시킨다.
- 봉인 검사가 원격으로 수행됨에 따라 세관에서의 컨테이너 통관속도를 높여준다.
- 전자 봉인이 선하증권, 주목적지 항만, 적하품목과 같은 정보를 포함함에 따라 적하 정보에 대한 빠르고 정확한 확인이 가능하다.
- 해운선사가 전반적인 운송체인을 따라 컨테이너 이동을 추적함으로써 높은 효율성을 가져다준다.

컨테이너 전자 봉인과 관련된 시장규모에 대한 예측은 거의 없는 상황이나 Frost & Sullivan에 따르면, 2006년 세계 컨테이너 봉인·모니터링 시장 규모가 3억 1천만 달러에서 2013년 5억 9,920만 달러로 확대될 것으로 전망되었다.

(3) 컨테이너 보안 장치(CSD) 시장

2006년 10월부터 시행되고 있는 미국 ‘항만보안법’에 따라 이르면 내년부터 미국에 수출하는 기업들은 컨테이너마다 미국 세관이 인정한 보안장치를 장착해야 한다. 현재로서는 전자 태그 또는 컨테이너 보안장치(CSD)가 표준 보안장치가 될 가능성이 높다. 특히, 최근 미국 하원을 통과한 ‘화물안전보안강화법’이 발효되면 이르면 2010년부터 미국으로 수출하는 모든 화물에 대한 사전 검색제도가 실행될 가능성이 크다. 미국 정부는 이를 준수한 화물에 대해선 미국 내 ‘신속 통관’ 혜택을 줄 계획이지만, 그렇지 못한 화물에 대해선 미국 내 하역 항에서 컨테이너 당 3~7일이 걸리는 정밀검사와 함께 2,000달러의 검사 수수료 및 창고료도 부과할 계획이다. 우리나라의 경우 미국과 컨테이너 보안협정(CSI)의 체결에 따라 2003년부터 부산항에서 미국 수출 컨테이너 화물에 대한 사전 검색제도를 시행 중에 있는데, 2007년 11월부터 부산항 감만 터미널에서 100% 검색 시범사업을 실시하고 있다.

향후 국내 CSD 시장 규모를 정확히 산출하는 것은 어려운 일이지만, 우리나라의 대미 수출 화물량을 기준으로 할 때, 부산항에서만 최소 1천억 원 이상의 비용

이 발생할 것으로 분석된다. 한국무역협회는 미국으로 수출되는 컨테이너 화물에 대한 100% 검색이 실시될 경우 부산항의 2006년 미국 발 수출 컨테이너 화물량 140만TEU를 기준으로, 시간당 150 TEU를 처리하는 50억 원 상당의 X-레이 검색대를 15대 구입해야 하므로 X-레이 검색대 구입에만 750억 원이 소요될 것으로 추산하였다. 이와 함께, 컨테이너마다 장착해야 하는 보안장치의 1회 사용료가 20~30달러 수준이므로 보안장치 구입비용에 연간 2,800만~4,200만 달러가 소요될 것으로 예상하였다. 다만, 초고속 컨테이너 검색기의 경우에는 차량이 검색기를 통과하는 과정에 검색이 이루어짐에 따라 운전자가 방사능에 노출될 가능성에 대한 논란이 제기될 수 있으며, 아직까지 장비의 해상도가 낮기 때문에 실제적인 적용은 다소 지연될 가능성도 있다.

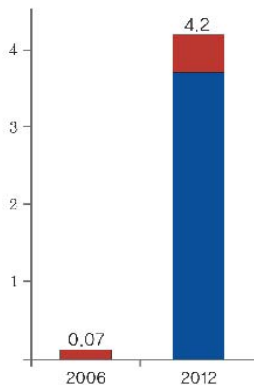
(4) 스마트(SMART) 컨테이너 시장

최근 미국 국토안전부(DHS : Department of Homeland Security)는 전략 컨설팅/시장 조사 기관 Homeland Security Research와 해운 물류 컨설팅 기관인 North River Consulting Group이 공동으로 수행한 조사 결과를 바탕으로 향후 대량살상무기(WMD)가 해상을 통해 밀매될 가능성이 높다고 판단하고, 이러한 위험성을 제거하기 위한 스마트 컨테이너의 유용성을 강조하고 있다.

<그림 5-3>

스마트 컨테이너 시장 현황과 전망

[스마트 컨테이너 시장규모(10억달러)]



[부문별 컨테이너 시장규모(백만달러)]



자료 : Homeland Security Research

이 보고서에 따르면, 스마트 컨테이너 산업은 추후 2004년에서 2012년까지 약 60배 성장하여 시장 규모가 2006년 7천만 달러에서 2012년에는 42억 달러에 이를 것으로 예측하였다. 또한, 2006년과 2012년 사이에 해운 컨테이너 보안 분야에 120억 달러가 지출되고, 지상용 커맨드, 컨트롤 통신 인프라에 약 7억 달러가 추가적으로 지출될 것으로 전망하였다.

3) 물류보안산업의 적용 부문

물류보안에 영향을 끼치는 핵심 요소에 근거하여 물류보안 적용산업은 크게 6가지로 구분될 수 있다.

(1) 시설관리 부문

화물이 제조되는 생산지 시설을 포함하여 화물이 재구성되거나 적재, 혼재, 혹은 환적을 위해 저장되는 주요 시설에 대한 보안 분야이다. 시설 자체에 대한 Fence 등의 물리적 통제를 포함하여 출입통제, 시설 모니터링, 창고 레이아웃 등에 관한 분야가 시설관리 분야에 해당한다. 이와 관련하여 물리적 통제를 위한 통제 장비, 출입통제 시스템, 시설 모니터링 관련 장비 및 소프트웨어 등을 대상으로 하는 산업이 포함된다.

(2) 화물관리 부문

화물관리 분야는 화물과 화물 적재용기에 대한 보안을 주요 대상으로 한다. 화물에 대한 위법적 접근이나 침입을 예방하고 감지할 뿐 아니라 이를 실시간으로 모니터링 할 수 있는 장비 및 소프트웨어 솔루션 등의 산업이다. 구체적으로 화물 검색시스템, 화물 위치추적 및 모니터링 시스템, 화물침입 방지시스템이 이러한 분야에 해당된다.

(3) 인적관리 부문

물류 전반에 걸친 시설과 프로세스를 관장하는 인적관리 부분도 보안의 중요한 영역에 속한다. 화물과 화물관련 시설에 직간접적으로 접근하는 직원들의 과거 경력검사, 보안과 관련된 교육, 조직 내에서의 물류보안관련 역할과 책임에 관한 훈련도 물류보안 분야에서 활용 가능한 산업이다. 이때, 보안관련 정보의 유포 및 공유에 대한 기본 원칙이나 조직 내 보안의식을 함양시킬 수 있는 조직문화 구축에

대한 교육관련 컨설팅도 인적관리 분야에서 적용할 수 있는 산업이라 할 수 있다.

(4) 정보 및 커뮤니케이션 관리 산업 부문

정보 및 커뮤니케이션 관리 분야는 보안 중 특히 정보에 대한 보안을 포괄하는 분야이다. 이에는 단순히 기업과 관련된 내부 정보의 비인가자 접근 금지와 같은 협의의 보안 외에 보안관련 정보의 질적 수준관리, 화물에 대한 정보 및 관련 사항에 대한 유지 관리, 고객 혹은 공급사슬 파트너들과의 보안관련 데이터에 대한 호환성 관리, 보안관련 데이터 관리를 위한 국제표준의 활용 등이 포함된다. 단순한 시스템의 개발 외에 보안이라는 특수성을 고려한 정보시스템의 관리 산업이다. 보안과 관련된 정보의 상호 호환성을 확보하기 위한 국제표준 기반의 인터페이스 개발 등의 사업도 고려해 볼 수 있다.

(5) 비즈니스 네트워크 및 기업보안 관리시스템 부문

물류보안 자체는 어느 단일 기업의 책임과 역할만으로는 해결될 수 없는 책임의 공유(Shared Responsibility)로 간주되기 때문에 이러한 비즈니스 네트워크 관점에서의 보안 관리가 필요하다. 따라서 기업의 물류보안 전반에 걸친 총체적 보안 관리 시스템 외에 물류상의 파트너에 대한 보안 평가 시스템도 상당한 가능성을 가진 사업 분야이다. 아울러 보안과 관련된 공공측면에서의 다양한 구상(Initiative)과 강제적 요구사항 등을 고려할 때 민간분야의 보안시스템과 공공분야의 보안시스템을 상호 연동해서 운용할 수 있는 민관보안협업 시스템 혹은 관련 인터페이스의 개발도 중요한 잠재력을 가진 사업으로 판단된다.

(6) 위기관리 및 재난복구 관리 부문

현재 논의되고 있는 물류보안 관련 법적 규제와 강제이행사항, 민간에서의 자발적인 노력들을 살펴보면 대부분 보안위험에 대한 조기 감지와 보안 위험의 예방에 주로 주안점을 두고 있다. 그러나 현실적으로 보안과 관련된 문제를 100% 완벽하게 방지하지 못한다는 사실을 감안하면, 보안관련 위기 발생시 이를 관리하고 신속한 복구를 지원하는 분야에 대한 수요가 높아짐은 자명한 사실이다. 따라서 기업 활동의 지속성 관리(Continuity management)를 위한 계획, 구체적이고 공식적인 보안관련 전략 수립, 문제 혹은 위기 발생 시 비상대책본부의 운영에 관한 매뉴얼, 재난복구계획(Contingency plan) 등과 같은 분야의 컨설팅과 관련 시스템 솔루션 분야도 보안을 활용한 산업으로 고려될 수 있다.

4) 주요 물류보안 기술 발전 및 경쟁력

(1) 컨테이너 봉인장치

컨테이너 봉인장치 기술은 과거의 단순 개폐 여부의 단순 정보에서 점차적으로 정보량을 확대해 나가는 방향으로 진행되고 있다. 봉인장치는 바코드를 활용한 봉인 장비들이 점차적으로 RFID를 기반으로 한 전자 봉인장비로 전환되고 있다. 전 세계적으로 전자 봉인장치(electronic seals)를 생산하여 판매하고 있는 기업들은 소수에 불과한데, 주요기업은 6개, 즉 Arbic Berhad, Harcor Security Solutions, Hi-G-Tek Ltd, Leghorn, Unisto Limited 등이 있다. 그러나 현재 한국의 기업이 전자 봉인장치를 제조하고 있는 기업은 없는 것으로 조사되었다.

<표 5-3>

봉인장치 생산기업별 기술보유 현황

기 명	Indicative Seals	High-Security Seals	Locks	Electronic Seals
Arbic Berhad	○	○	-	○
Acme Seals Limited	○	○	-	-
Alpha Cargo Technology, LLC	○	○	-	-
American Casting & Manufacturing Corporation	○	○	-	-
CGM Security Solutions, Inc	-	○	○	-
E.J. Brooks Company	○	○	-	○
Hi-G-Tek Ltd	-	-	-	○
Harcor Security Seals Pty	-	○	-	○
Leghorn, srl	-	○	○	○
OneSeal A/S	-	○	○	-
Relcor Inc.	-	○	○	-
Sealock Security System Inc.	-	○	○	-
Shanghai Xinfan Container Fittings Co., Ltd	○	○	-	-
Stoffel Seals Corporation	○	○	-	-
TydenBrammall	○	○	-	-
Transport Security, Inc	-	○	○	-
Unisto Limited	-	○	-	-
Universeal Group	-	○	-	-
Wenzhou Yanjiang Security Seals Co, Ltd.	○	○	-	-

자료 : Frost & Sullivan

(2) RFID를 활용한 전자 봉인장비

RFID를 활용한 전자봉인 장비를 개발하여 판매하는 시장은 사실 GE와 SAvi로 양분되어 있다. 이 기업의 제품들은 이미 기술적인 검증 단계를 거쳐 실제로 사용되고 있다. 다만 문제는 RFID의 태그 가격을 낮추는 것으로 알려지고 있다. 따라서 기술개발 방향은 태그의 가격을 낮추는 방향으로 연구가 진행되고 있다고 할 수 있다.

<표 5-4>

RFID를 활용한 전자 봉인장비 생산기업 및 제품

기업 명		제품
컨테이너 보안 장비	GE Security, Inc	CommcerceGuard CSD, readers and software
	Savi Technology, Inc	Savi Sensor Tag ST-673, 674, and 675; Echopoint readers; SaviTrack software
	International Business Machines Corporation	Intelligent Trade Lane, Tamper-evident embedded controllers(TREC)
	Impeva Labs, Inc	Global Sentinel
	L-3 Communications Corporation	Advanced container security device
	Science Application International Corporation	Advanced container security device
	SeaAway	SeaAway CSD
컨테이너 추적 장비	Savi Technology, Inc	SaviTags ST-604, 605, 654, 656
	WhereNet Corp	WhereTag
	NaviTag Technologies, Inc	NaviTag
	Altobridge	Global Integrated Maritime Monitoring w/AM Gateway Platform
	Asset Tracking Logistics and Securitiy LLC/MPS, Inc	AM-11C
	Axcess Inc	ActiveTag
	ContainerTrac, Inc	Terminal Automated Tracking System
	Hi-G-Tek Ltd	DataTag
	iControl Incorporated	iDAC, iGate, iView
	Identec Solutions, Inc	ILR I-D2, ILR I-Q, ILR I-B tags
	Lorantec Systems, Inc	RTC 1000
	Fairfield Industries, Inc	RFTrax Asset Management Platform Systems
	Transport Security, Inc	Enforcer Trax 200

자료 : Frost & Sullivan

(3) 화물 검색장비

방사선 탐지장비 기술에서 핵물질을 감지하기 위해 폴리비닐 톨루엔(Polyvinyl toluene)을 사용하여 광자(photons)를 탐지하는 방법이 20년 이상 사용되어 왔다. 그러나 이 방법은 신뢰도가 낮아 요오드화나트륨(sodium iodide) 혹은 게르마늄(germanium)을 이용한 새로운 기술이 개발되고 있다. 미국 국토안보부에서는 새로운 기술에 대한 심층 분석을 한 후 게르마늄을 이용하는 방법을 표준으로 채택하는 방향으로 진행하고 있다.

현재 컨테이너 내부를 영상으로 검색하는 장비는 X-선 혹은 감마(Gamma)-선을 이용하는 기술이 활용되고 있으나, 낮은 투과성으로 인해 100% 검색은 불가능하며 이를 보완하기 위해 수작업을 병행하고 있어 검사 속도가 낮은 단점이 있다. 이 문제를 해결하기 위한 많은 연구들이 진행되고 있고, 16인치 두께의 철을 통과하는 투과성 기술을 확보하여 검사시간을 줄이는 것이 연구의 일차적 목표로 알려지고 있다.

<표 5-5> 방사선 탐지 및 내부영상 검색장비 생산기업 및 제품

기업명		생산제품
방사선 탐지장비	SAIC	Exploranium line of radiation portal monitors
	CANBERRA Industries	RadSentry Radiation Portal Monitor(RPM), Advanced Spectroscopic Portal
	Raytheon Company	Advanced Spectroscopic Portal
	Thermo Fisher Scientific, Inc	ASM 3000SE, ASP
내부영상 검색장비	Science Application International Corporation	VAIC line of non-intrusive inspection systems
	America Science and Engineering, Inc	Z Backscatter Van, Z portal, OmniView Gantry, MobileSearch, etc
	L-3 Communications Corporation	CX-3800G, CX9000F, CX600R Fixed site X-ray systems, etc
	Rapiscan Systems	VEDS, Eagle, GaRDS Inspection Systems

자료 : Frost & Sullivan

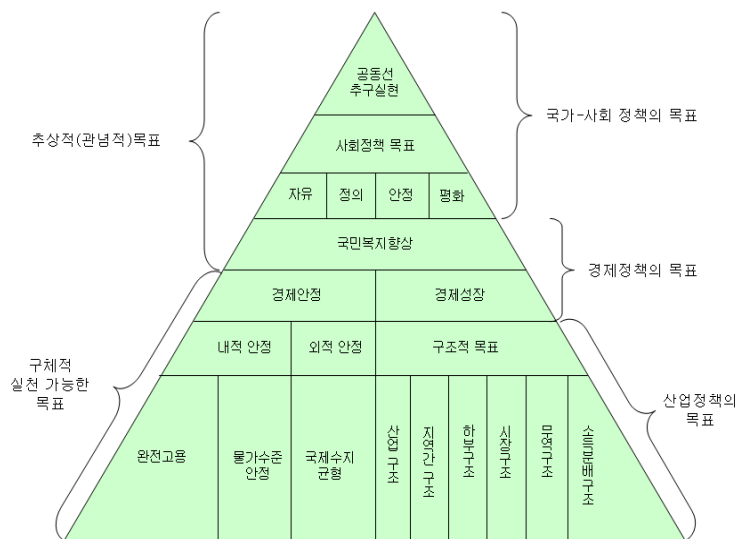
2. 물류보안산업 지원·육성 방안

1) 정책 목표와 수단

산업정책은 한 가지 목표를 추구한다기보다 여러 가지 형태의 개별적 목표를 동시에 추구하는 것이 일반적이다. 그리고 어떤 정책의 최종목표는 다른 어느 것의 중간 목표일 수도 있고, 더 하위목표가 될 수도 있다. 말하자면 산업정책의 최종목표라 할 수 있는 최적배분이라는 것도 공동선의 실현이라든지 홍익인간의 실천이라는 사회공동체의 목표에 비하면 하나의 수단일 수도 있으며 반대로 어느 정책 목표를 달성하기 위한 수단은 또 다른 정책의 목표가 될 수 있다. 예를 들면, 기계제조업에 대한 정부의 세제상 지원은 기계공업의 육성이 일차적 목표이지만, 이 목표 또한 공업화 내지 경제성장정책의 수단에 불과할 것이다. 또한 경쟁적 시장질서의 유지는 산업조직 정책의 최종목표이나 자원의 최적배분이라는 산업정책의 입장에서는 한 수단에 불과하다는 것이다.⁹¹⁾

<그림 5-4>

경제 및 사회정책의 목표-수단 피라미드



자료 : O. Issing(ed), Allgemeine Wirtschaftspolitik, Muenchen, 1982, p. 8.

91) 이갑수, 「글로벌시대의 산업정책론」, 도서출판 대명, 2007.

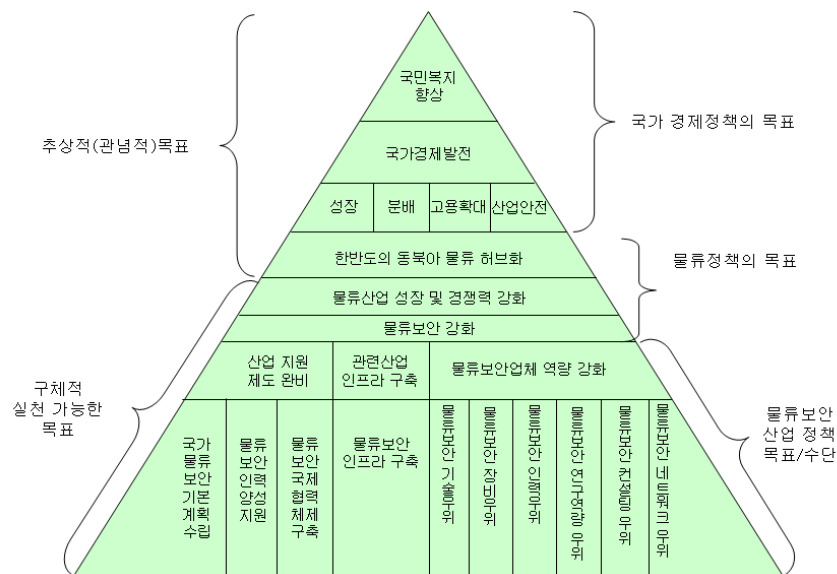
이러한 논리를 정책의 목표와 수단에 내재하는 ‘목표 피라미드’라고 한다. 다음 <그림 5-4>는 산업정책이 어떠한 목표를 가지고 있는지 또 스스로 경제·사회정책의 수단으로서 어떠한 역할을 하고 있는가를 나타내고 있다.

경제 및 사회정책의 목표-수단 피라미드를 물류보안산업 육성정책에 적용하면 다음과 같다. 물류보안산업 육성정책의 1차적 목표는 물류산업의 성장 및 물류경쟁력 강화에 있고, 상위 목표는 한반도의 동북아 물류 허브화 정책이라고 할 수 있다. 그리고 이러한 물류보안산업 정책의 근본적 목표는 국가경제 발전과 국민생활 및 복지 향상이라고 할 수 있다.

물류보안산업의 육성을 위해서는 물류보안산업 지원제도 완비, 물류보안산업 인프라 완비, 물류보안업체 역량강화 등이 1차적으로 요구된다. 그리고 물류보안산업의 지원제도는 국가물류보안 기본계획 수립, 물류보안 인력양성지원, 물류보안 국제협력체제 구축 등을 들 수 있다. 그리고 물류보안업체의 역량 강화는 물류보안 기술개발, 장비, 인력, 연구역량, 컨설팅, 네트워크 등이 다른 국가보다 우위에 있도록 해야 한다. 이상의 내용을 도식화하면 <그림 5-5>와 같다.

<그림 5-5>

물류보안산업 육성정책의 목표와 수단



한편, 물류보안의 강화는 물류비용의 상승을 가져와 물류경쟁력 강화라는 목표와 상충될 수 있다. 이른바 ‘목표간 충돌’(Zielkonflikt)이다. 목표간 충돌이 발생하는 경우 이것을 조정하기 위해서는 ‘차선의 이론’(theory of second best)을 동원하기도 하지만, 결국 정치적으로 해결⁹²⁾을 하게 되는 경우가 많다. 정치적 해결이 경제적으로는 최선이 아니지만 유일한 해(solution)가 된다는 뜻이다.

그리고 정책목표 사이에는 목표간 충돌 외에도 목표간 보완관계(Zielkomplementarität), 목표간 대체관계(Zielsubstitutät), 목표간 중립관계 등이 발생한다. 목표간 대체 관계는 목표간 모순이 존재한다는 것으로 물류보안의 강화와 물류 속도 향상과의 관계가 예가 될 수 있다. 목표간 보완관계는 목표간 조화라고도 하는데, 물류보안의 강화와 화물의 안전한 물류서비스 제공이 동일한 의미로 사용되는 것과 같다. 목표간 중립관계란 여러 목표간 아무런 상관관계가 없는 것을 의미한다.

2) 물류보안산업 육성을 위한 산업구조정책

‘현재 존재하지 않는 미래산업이나 아주 취약한 산업이라도 시장여건의 변화, 기술진보의 요인에 의해 장래성이 있다고 판단되는 경우에는 산업생산의 증가나 발전을 도모하는 정책을 취할 수 있다. 이러한 목표를 가진 산업정책을 구조형성 정책 또는 구조발전정책이라 한다. 그리고 이러한 목표를 실현하기 위하여 보통 과학·지식산업의 육성, 기술교육의 강화 등 하부구조(infrastructure)의 확충이 동시에 추구된다.’⁹³⁾

한편 이러한 산업구조형성 정책목표를 추구하는 과정에서 다음과 같은 정책 실패를 경험할 수 있는 위험이 존재한다. 첫째, 장래성이 없는 유치산업을 위해 과중한 투자를 행할 우려가 있다든가 국가체면을 위해 경제성이 없는 산업에 투자를 행할 우려가 그것이다. 둘째, 구조형성정책이 자칫 사양산업에 적용될 우려가 있다. 경제압력단체의 강력한 로비에 직면하여 정책당국의 산업정책이 이러한 방향으로 가지 않는다는 보장이 없다. 이러한 위험에도 불구하고 산업구조 형성정책은 선·후진국을 막론하고 가장 중요한 목표가 되고 있으며, 그 이유는 경제성장의 가장 효율적인 수단이며, 특히 개발동상국의 국가발전에 중요한 도구로 인식되기 때문이다.

일반적으로 산업구조 형성정책의 수단은 i) 하부구조의 구축, ii) 성장잠재력

92) 여기서 정치적 해결이란 경제학적 접근이나 방법을 벗어나는 해결책을 의미한다.

93) 이갑수, 「글로벌 시대의 산업정책론」, 도서출판 대명, 2007.

개발, iii) 기술혁신 등이 거론되고 있다.

(1) 하부구조의 구축

하부구조란 경제주체의 경제행위를 도와주는 모든 물적·비물질적 자산의 총칭으로 요힘센(R. Jochimsen)에 의해 강조되어 왔다. 요힘센에 따르면 하부구조는 존재 자체로 인해 한편으로는 지역간·부문간 존재하는 생산요소에 대한 보수의 차이를 해소할 수 있고, 또 경제적 통합을 실현하고 다른 한편으로는 국민경제의 성장이 촉진되기 때문에 매우 중요하다. 이러한 하부구조는 상부구조에 대한 대충으로 눈에 보이는 경제행위 및 성과를 우회적·장기적으로 개선하는 눈에 보이지 않는 모든 자산으로 제도적·인적 요소까지 포함될 수 있다. 따라서 여기서 말하는 하부구조는 일반적으로 이야기되는 사회간접자본(SOC)의 개념보다 더욱 포괄적이다.

생산 활동에서 간접자본의 역할은 매우 중요하다. 사회적으로도 사회적 효율을 전반적으로 제고시키는 사회적 간접자본의 역할은 매우 중요하다. 그것은 장기적으로 국민경제의 효율을 좌우하기 때문이다. 이는 사회간접자본의 부족으로 성장의 애로를 겪는 나라들이 많다는 데서도 알 수 있다. 최근 우리나라가 겪고 있는 교통체증으로 GDP의 손실이 발생하고 있다는 사실에서도 사회간접자본이 어느 정도 경제효율에 영향을 주는가를 알 수 있다.

물류보안산업의 육성을 위한 하부구조는 매우 광범위하다. 물류보안산업은 기본적으로 물류산업의 영역에 속하기 때문에 물류관련 인프라가 물류보안산업의 기본적인 인프라에 속한다. 그리고 보안의 기능을 할 수 있도록 하는 시스템이 부가된다. 물류보안의 기능을 담당하는 시스템은 화물추적장비 및 네트워크, 화물검색 및 분석 시스템, 항만·공항·철도·ICD 등에서의 물류보안시설, 물류보안 통신망 등을 들 수 있다. 이러한 물류보안 하부구조는 개별 민간기업의 업무범위를 넘어서는 것으로 이를 구축하기 위해서는 국가 또는 관련 단체에서 기획, 설계, 시공, 운영하는 등 모든 업무 과정을 통제해야 한다.

(2) 성장 잠재력 개발

산업정책이란 다르게 표현하면 적극적인 경제성장 정책이다. 국내외 시장개발을 통해 개별산업의 성장을 도모하고, 다른 한편으로는 기술혁신과 잠재성이 없는 산업의 구조조정을 통해 국민경제 전반의 생산성을 제고하는 것이 산업정책의 목표이다. 따라서 구조형성 정책은 가장 중요한 산업정책의 하부구조가 되고 있다.

왜냐하면 국민경제 전체의 성장 잠재력을 제고하고 미래 지향적 산업구조를 조성해 나가는 정책이기 때문이다.

성장잠재력 개발 정책은 산업의 미래 성장가능성을 보고 정책적으로 산업을 육성하는 것을 말한다. 과거 일본을 비롯해 급속한 산업성장을 달성한 국가는 대부분 산업 잠재력 개발 정책을 구사했다. 이 때 성장 잠재력이 높은 산업은 i) 수요 탄력성이 높은 산업, ii) 산업의 전·후방 연관효과가 큰 산업, iii) 기술파급효과가 크고 기술집약적인 산업, iv) 내부경제(규모의 경제, 학습효과)가 큰 산업 등이 선정되었다.

우리나라에서도 1980년대 정책자문기구를 통해 i) 국가기간산업(국민경제에 영향이 큰 산업), ii) 기술인력 집약산업, iii) 에너지 및 자원절약산업, iv) 해외시장전망이 밝은 산업이라는 기준을 통해 10대 전략산업을 선정하여 육성했다. 그 후 첨단기술의 중요성이 증대하자 기술적 요인을 중심으로 7대 전략산업을 발표하였다. 7대 산업에는 정밀전자, 메카트로닉스, 정밀화학, 신소재, 생명공학, 항공우주, 해양·자원 산업이 속한다. 그리고 이들 산업의 육성을 위해 정부는 금융지원(특히 수출금융지원), 인력양성 지원사업 전개, 세제지원, 택지개발 지원, 기술개발 지원, 인프라 구축사업 등을 전개해왔다.

물류보안산업은 물류보안제도의 확산에 따라 새롭게 등장한 산업이다. ‘세계의 물류보안시장 규모는 1,600억 달러(약 152조원)에 달할 정도로 커졌고, 연평균 7~8%씩 성장하고 있는 유망산업이다.’⁹⁴⁾ 그리고 컨테이너 화물 검사장비와 방사능 탐지장비, RFID와 화물 추적장치 등을 포함한 ‘스마트 컨테이너’ 시장은 향후 40억~50억 달러 시장으로 확대될 전망이다.⁹⁵⁾ 그러나 우리나라의 물류보안 관련 기업의 시장 참여는 아직 초보적인 단계에 있다. 물류보안 시장을 주도하고 있는 미국의 GE나 사비와 업무협정을 맺은 일부 업체만 시장에 참가하고 있다. 물류보안산업의 영역은 물류산업과 보안산업이 기본적으로 결합하고, 첨단과학정보기술도 필요로 한다. 따라서 사업의 범위와 영역이 매우 넓어 우리나라의 물류 및 IT 업체가 참여할 때 성장 가능성이 매우 높은 부문이다.

따라서 정부에서는 물류보안산업의 성장 가능성을 고려하여 다양한 지원 정책을 개발해야 한다. 물류보안산업을 육성하기 위해서는 산업 성장 초기에 다양한 지원이 필요하기 때문이다. 지원 대상분야는 물류보안 장비기술 개발지원, 물류보

94) 루이스 파커(GE Security 부문 사장)의 인터뷰 내용(<http://tong.nate.com/raccoon1128/29104954>)

95) 최재선, “최근의 물류보안 강화 동향”, 「물류보안 대책 마련을 위한 대토론회」 자료집, 한국무역협회·한국해양수산개발원, 2006. 10. 17. p. 23.

안 정보기술 개발지원, 물류보안 인증 시스템 개발지원 등을 고려할 수 있다. 지원 방안은 이들 각 분야의 기술을 개발하는 업체에 대한 세제상의 지원, 인력개발 양성지원, 수출금융 제공, 물류단지 입주 지원 등을 고려할 수 있다.

<표 5-6>

GE 물류보안 담당사장의 인터뷰 기사

三星물산과 물류보안 합작 Louis Parker GE Security CEO

<http://tong.nate.com/raccoon1128/29104954> 주소복사

2006.11.20 16:07

[신고하기](#)

三星물산과 물류보안 합작 Louis Parker GE Security CEO Interview
"Terror 공포로 보안없이 수출도 어려워"

"테러의 위험이 전 세계로 확산되면서 공항검색은 물론, 배로 실어나르는 무역 화물에 대해서도 보안검색이 강화되고 있습니다. 보안 없이는 수출도 어렵게 된 거죠."

최근 삼성물산과 물류 보안사업 분야의 합작계약 체결을 위해 방한한 루이스 파커(Louis Parker-52) GE 시큐리티 사장은 "보안산업은 세계시장 규모가 1600억달러(152조원)에 달할 정도로 커졌고, 연평균 7~8%씩 성장하고 있는 유망산업"이라고 강조했다.

GE 시큐리티가 삼성물산과 협력한 분야는 아시아 12개국 수출 컨테이너의 보안산업이다. 폭발물이나 마약이 수출 컨테이너에 담겨 이동하는 것을 막고, 화물의 이동경로를 추적해 도난과 분실을 막아준다. 파커 사장은 "미국에선 최근 '항만보안법'이 통과됐다"면서 "보안장치를 부착한 컨테이너는 보다 빠르게 화물검색을 통과하게 될 것"이라고 말했다.

공항 보안시스템 개발도 주요 투자분야다. 최근 의료분야에서 사용되는 컴퓨터 단층촬영기를 활용, 항공기 승객들과 수하물에 포함된 폭발과 마약을 정밀하게 검색하는 '폭발마약 감지 시스템'을 개발했다.

"공항 보안검색의 문제는 승객들이 신체검사 때문에 불편을 겪고, 검사해야 할 짐이 너무 많다는 점입니다. 검색견(犬)이 있긴 하지만, 30분 이상 검색작업을 계속하기 힘들죠. 새로 개발한 감지 시스템은 24시간 가동할 수 있고, 마약을 감지했을 경우 마약의 종류까지 알려줄 정도로 정확성을 높였습니다."

그는 보안산업이 갈수록 커지고 있다고 말한다. "자녀가 학교에서 집으로 안전하게 돌아왔다는 사실을 직장에서 알리는 부모의 휴대전화에 문자로 통보해 준다든가, 노부모의 외출과 귀가 여부를 알려주는 것처럼 보안산업은 인간의 생활을 보다 편하게 해주는 분야로도 발전하고 있습니다."

파커 사장은 펜실베이니아 대학과 하버드 비즈니스 스쿨 출신으로, IBM과 모건스탠리를 거쳐 96년 GE에 입사했다. GE의 기업보안사업 사장을 거쳐 올해 초 GE시큐리티 CEO(최고경영자)가 됐다.

김종호 기자 [tellme@chosun.com]

(3) 기술혁신

물류보안산업에서 기술혁신은 제품기술에 대한 보안당국의 인증과 수요자의 가격 호응도를 기준으로 이루어져야 한다. 물류보안장비나 기술은 개별기업에서

사용하지만 물류보안당국의 인증이 필요하기 때문에 일차적으로 물류보안당국의 기준을 충족해야 한다. 현재 물류보안에 관한 기술은 대부분 미국의 GE, 사비 등에서 독점하고 있으나 이를 능가하는 기술적인 성능과 안정성을 구비하는 기술력이 필요하다. 더불어 물류보안장비와 기술이 확산되기 위해서는 가격이 저렴해야 한다. 사실 물류보안당국의 인증을 받은 업체간의 경쟁은 기술보다 가격 경쟁력에 의해 결정될 수밖에 없다. 물류보안을 위한 절차가 소비자가 사용하는 제품이나 서비스의 수준과는 무관하기 때문이다.

한편 산업기술의 연구·개발이란 정책적 과제는 국내외적으로 경쟁이 치열해져간다는 인식하에 출발한다. 새로운 생산기술은 가격을 인하시키거나 제품의 질을 향상시키거나, 새로운 제품을 시장에 내놓음으로써 신수요를 창조하기도 한다. 산업의 성장 가능성(발전능력)은 산업기술의 발전과 함께 한다. 다시 말하면 어떻게 신 공정 기술이나 신제품을 개발하여 신속히 산업생산에 상용화할 수 있는가에 달려 있다고 할 수 있다.

시장경제 질서 하에서는 산업기술의 연구 및 개발, 새로운 상품과 공정의 개발은 일차적으로 기업의 책임이다. 그러나 국제경쟁력을 제고시키는 측면에서 해당 산업의 기술 잠재력을 배양시킨다든가 외부적 환경을 유리하게 이끈다는 것은 정부의 역할에 따라 좌우되기도 한다. 따라서 구조형성정책의 중요한 과제는 민간(기업)의 연구·개발 의욕을 자극하고 지원하는 일이기도 한 것이다.

일반적으로 한 나라의 산업구조형성을 위한 기술정책은 기술개발에 의해 경제적 위험이 존재하는 경우, 즉 R&D 투자와 예상되는 수익 사이 뚜렷한 비전이 없어 기업의 기술투자를 유치하기 어려울 때 그 의의가 크다. 더구나 그것이 중요 기간산업이라고 할 때 정부의 개입(구조형성적 기술정책의 실시)은 불가피한 것이다. 만약 정부의 적절한 대응정책 없이 특정산업의 기술혁신이 완만해서 구조형성이 지연된다면 이것은 정부의 중대한 과실이 아닐 수 없다.

한편 장래성이 있는 산업을 육성함에 있어 정부가 직접 산업기술을 개발하거나 지원하는 것도 중요하지만, 사회 전체의 지식이나 교육 수준을 제고시키는 문제도 중요하다. 대학의 기초연구, 직업교육 등은 산업기술개발의 외부환경으로 중요한 간접자본이 될 것이다. 이를테면 물류보안기술 개발을 위한 연구사업 등이 이에 해당한다.

3) 물류보안산업 부문별 지원 방안

(1) 컨테이너 전자 봉인장치

가. 컨테이너 전자 봉인장치 표준 확정

컨테이너 잠금장치 시장도 크게 변하고 있다. 지금까지 기계적인 봉인에서 물류 보안제도가 강화된 이후 전자적인 봉인장치 사용이 확대되고 있기 때문이다. 일반적으로 컨테이너에 제품의 선적이 완료되면 선적 장소에서 화주 또는 하역업체의 책임 하에 컨테이너의 봉인을 해왔다. 이는 화주와 운송인 사이에서 제품의 수량과 내용에 하자가 발생하지 않도록 하기 위함이다. 봉인을 위한 장치는 운송을 담당하고 있는 해운회사나 포워더 등에 의해 관리되며, 운송을 원하는 하주에게 봉인장치가 전달된다. 이때 각 물류업체마다 자사의 특성에 맞게 다양한 봉인장치 사양이 선택되어 사용되고 있다.

그러나 최근 물류보안이 강화됨에 따라 컨테이너 보안장치에 대한 국제 표준이 마련되고 있다. 이는 기존의 봉인장치가 운송과정에서 훼손, 파손, 개봉되는 경우가 있었고, 심지어 운송도중에 개봉된 후 재봉인이 되더라도 확인이 쉽지 않은 문제가 있었기 때문이다. 이러한 문제를 효과적으로 극복하기 위해 전자봉인장치(E-seal)가 개발되었고, 이에 대한 국제표준 규격이 2007년 5월 10일 ISO IC104/SC/WG2에서 결정되었다. 즉, 전자봉인장치에서 사용되는 전자 태그의 주파수를 433Mhz와 2.4Ghz를 모두 지원하는 ‘듀얼 밴드’로 채택하고, 전자봉인 리더기는 433Mhz와 2.45Ghz 중 하나를 지원하는 것이다. 그런데 ISO에서 추진하고 있는 표준이 미국의 항만보안법에 규정되어 있는 컨테이너 보안장치(CSD)와 다르다. 따라서 ISO와 미국의 표준의 통일 여부가 향후 문제점으로 지적되고 있다.

ISO에서 규정한 전자봉인장치 표준화 범위는 모두 Part 1~7로 구성되었으나, Part 5와 Part 6이 제외되어 최종적으로 5가지로 합의되었다. Part 1은 봉인 데이터의 송수신을 위한 데이터 링크 계층에서의 포맷을 정의하는데, 데이터 형태의 구성은 봉인/개봉의 날짜 및 시간, 봉인상태(open&unsealed, closed&sealed, opened), 배터리 상태, 프로토콜 ID 및 Version 등이다. 통신프로토콜은 Type A(433Hhz)와 Type B(2.45Ghz)로 구성된다. Part 2는 전자봉인장치의 응용 및 성능요구 조건을 정의하고 있다. 즉 봉인장치의 ID는 장치의 외부에 각인, 배터리 수명은 2년 이상, 개봉 및 봉인 날짜 및 시간 표시, 가독률 99.99%, 정확성 99.99% 등의 내용을 포함

한다.

그리고 Part 3은 전자봉인장치의 환경요인 요구조건을 명시하고 있는데, 온도 (최저 -40도, 최고 +70도), 물리적 충격 30g(11ms), 진동 3g(2시간), 습도 95%, 소금 물 속 1m 등에도 견뎌야 하는 것으로 되어 있다. Part 4는 데이터의 보호 및 장치 인증 규정을 정의하고 있다. 데이터 보호 측면에서는 비밀정보, 개방정보, 고정 데이터, 변동 데이터 등이 있으며, 인증은 물리적 및 전자 인증으로 구성된다. Part 7은 봉인장치의 물리계층의 프로토콜을 정의하고 있는데, Type A와 Type B를 함께 지원해야 한다.

<표 5-7>

ISO 전자봉인장치 표준화 범위

구 분	내 용	기 능
Part 1	Communication protocol	송수신을 위한 데이터 링크 계층에서의 포맷을 정의
Part 2	Application requirement	응용 및 성능요구 조건 정의
Part 3	Environmental characteristics	환경요인 요구조건 정의
Part 4	Data protection	데이터 보호 및 장치 인증 규정을 정의
Part 5	Sensor interfaces	표준화 범위에서 제외됨
Part 6	Message sets for transfer between seal reader and host computer	
Part 7	Physical layer status	물리계층의 프로토콜을 정의

자료 : 한국해양수산개발원

나. 전자봉인 장비 현황 및 문제점

컨테이너 전자봉인장치 기술은 433Mhz에 기반을 둔 미국의 록히드 마틴 그룹의 Savi Technology사와 2.45Ghz의 GE그룹이 양분하고 있다. ISO에서 전자봉인장치를 개발할 때 통신 프로토콜(communication protocol)에 사용되는 기술을 ‘듀얼 밴드’로 정함에 따라 기업체에서 원천기술 사용료, 즉 특허 사용료를 두 회사에게 지불하게 되었다. 특히 Savi사는 자신이 개발한 기술을 사용할 때 사전승인을 받도록 하는 조항을 포함하였다.

① Savi Technology

Savi Technology사는 ISO 18185 A Type인 443Mhz 대역을 지원하는 전자봉인장치를 개발하여 공급하고 있다. 현재 Savi사의 'QuickStart'에 대한 라이선스 프로그램에 참여하고 있는 업체는 Axess International(미국), Evigia Systems(미국), SAVR(미국), Envotech(말레이시아), Identec Solutions(호주), KPC(한국) 등 6개사가 참여하고 있다.

Savi사는 HPH(Hutchison Port Holdings)사와 싱가포르 투자회사인 테마섹 홀딩스, NOL, APL 및 싱가포르 에어라인, MOL, 오라클 등의 대형 물류업체와 솔루션 업체 등이 투자해 미국의 캘리포니아 서니베일에 설립한 민간회사였으나 1989년 미국의 대형 군수업체인 록히드 마틴에 인수되었다. 사비 사는 현재 미국 국방부와 북대서양 조약기구뿐만 아니라 영국과 덴마크 등 전 세계 국방관련 업체에서 군수품을 관리하는 사업에 참여하고 있다. 개발하고 있는 제품은 화물에 대한 전자 태그, 리더기, 데이터베이스에 정보를 전송하는 무선 네트워크 시스템, 고객에서 정보를 제공하는 소프트웨어 등이다.

② GE Security

GE사는 미쯔비시, 지멘스 등과 국제컨테이너보안협회(ICSO)를 창설하여 ISO 18185 B Type인 2.45Ghz 대역을 지원하는 전자봉인장치를 개발하여 공급하고 있다. GE사가 개발하고 있는 컴머스가드 컨테이너 보안 솔루션(Commerce Guard Container Security Solutions)은 컨테이너 내부에 자기적으로 부착되어 컨테이너 도어의 모든 개방 여부를 기록하는 CSD(Container Security Device)를 활용한다. 즉, 주요 지점에 설치된 소형 리더기가 CSD에서 컨테이너 개폐 기록을 전달 받아 Commerce Guard Data Center로 전송하는 방식이다. 공인된 화물 소유주, 물류업체, 정부기관은 세계 어느 곳에서나 인터넷 브라우저를 통해 정보를 안전하게 데이터 센터에 접근할 수 있다. 공인되지 않은 컨테이너의 개폐 기록은 화물 훼손으로 기록되어 관련자에 보고되어 효과적인 사후처리가 가능해진다. 또한 훼손 기록이 없는 컨테이너의 경우 수출입 항구에서 신속히 통관 처리될 수 있다. 화주는 데이터 센터를 통해 물류 망에서 움직이고 있는 화물의 위치 및 현재 상태에 대한 정보를 얻을 수 있다.

③ 문제점

컨테이너 운송에 전자봉인장치의 부착이 의무화되거나 일반화될 경우 물류비

상승이 우려되고, 기술종속이라는 문제가 발생할 가능성이 높다. 우리나라의 경우 이에 관한 원천기술을 확보하지 못하고 있기 때문이다.

i) 물류비 상승

미국이 전자 태그(RFID) 부착을 강행하면 화주와 물류업체는 추가적인 비용 부담으로 원가 상승이 불가피하게 된다. 능동형 RFID의 경우 수동형 제품보다 가격이 비싸다. 현재 컨테이너 박스를 한국에서 미국으로 운송하는 운임은 약 250만~350만원이지만, 433Mhz 대역 능동형 RFID를 부착할 경우 추가로 20만~100만원이 소요되는 것으로 조사되었다.

한편, 물류업체는 RFID 태그 탈·부착을 위한 인프라를 구축해야 하며 이에 대한 시설투자는 화주에게 전가될 가능성이 있으며, 화주는 통관의 편의를 위해 태그 비용을 부담하지 않을 수 없다. 이는 물류비 상승에 따른 제조 원가로 이어질 수밖에 없다.

ii) 기술종속 우려

433Mhz 대역의 능동형 RFID 기술은 미국의 Savi 테크놀로지 사가, 2.45Mhz 대역은 GE사가 주도하고 있고, 현재로서는 대체할 만한 제품이 없는 상황에서 Savi 혹은 GE사의 제품을 이용할 수밖에 없는 것으로 분석되고 있다. 특히 Savi사는 세계 각국의 항만과 연계하여 태그를 임대하는 방안을 추진하고 있다. 비싼 가격에 태그를 구입하지 않고 10만원 정도에 임대할 경우 미국행 컨테이너에는 Savi사의 제품이 일반적으로 사용되는 상황이 발생할 수도 있다.

다. 전자 봉인장치 기술 육성방안

국제표준화기구(ISO)는 컨테이너 전자봉인장치에 대한 국제표준을 채택하였다. 국제표준은 RFID 태그 주파수를 433Mhz와 2.45Ghz를 모두 지원하는 듀얼밴드로 확정하였고, 리더기의 경우는 하나만 지원하면 되는 것으로 되어 있다. 그리고 전자봉인의 RFID 태그에 기록될 데이터는 국제규정에 따라 단순히 컨테이너의 봉인 여부에 관한 사항만 저장되기 때문에 데이터 관리문제는 심각하지 않은 것으로 판단된다. 세계선주협회에서는 전자봉인장치가 일회성으로 개발되어야 하고, 가격이 컨테이너 당 10달러 이하로 설정되어야 한다고 주장하고 있다. 따라서 향후 전자봉인 장비와 관련해서는 RFID의 인식률 제고, 태그 가격인하 등을 위한 기술 개발이 주안점이 될 것으로 예상된다.

이러한 관점에서 볼 때 Savi사와 GE사는 이미 전자봉인장비 제품을 개발하여 보급하고 있다. 따라서 우리나라는 Savi사나 GE사와의 기술격차를 감안하여 요소 기술에 대하여 자체로 기술 개발을 할 것인지 아니면 기존에 개발한 제품을 활용 할 것인지에 대한 정책이 필요하다.

현재 Savi사는 세계 최대 터미널 운영업체인 허치슨과 합작으로 주요 항만에 RFID 인프라를 설치, 운영하고 있다. 또한 한국의 KPC사는 Savi사와 라이선스 프로그램에 참여하여 기술을 개발하고 있다. GE사는 화주 중심의 컨소시엄을 구성하여 시장 진입을 시도하고 있고, 삼성물산의 경우 GE사와 이미 판권계약을 체결하고 올해 부산항과 미국 롱비치 항로를 대상으로 시범운행을 하기도 하였다. 따라서 우리나라가 기술개발을 할 경우 Savi사나 GE사의 제품보다 성능이 우수하거나 가격 경쟁력에서 우위를 확보해야 개발 후 시장성을 확보할 수 있다.

우리나라에서 기술개발을 추진할 경우 라이선스 보호가 중요할 것으로 판단된다. 따라서 ISO/IEC 18185에 관련된 기술개발과 더불어 국제 특허확보에 적극적으로 대응하는 체계가 필요하다. 비록 통신 프로토콜 부문에서는 Savi나 GE사에게 원천기술 사용료를 지불해야 하나, 인식을 제고, 온도, 습도, 충격, 진동, 방수/염수 규정, 배터리 수명 등의 부분에서 가격을 낮추면서 성능이 뛰어난 기술이 개발된다면 이를 적극적으로 보호해야 하기 때문이다. 현재 한국 RFID/USN 협회에서 해외특허 공동대응협의체를 구성하고 있으나, 정부차원에서도 이를 적극적으로 지원하는 방안이 필요하다. 또한 산학연 협동 체제를 구축하여 원가를 낮추는 기술 개발과 이를 위한 저금리 자금 지원이나 파이낸싱 등을 정부차원에서 지원할 필요가 있다고 판단된다.

(2) 컨테이너 화물 검색기

가. 컨테이너 화물 100% 검색 의무화

2007년 8월 3일 부시 미 대통령은 미국으로 반입되는 모든 컨테이너 화물에 대한 100% 사전 검색을 의무화하였다. 이 법률의 명칭은 ‘9.11 테러대책 위원회의 권고를 이행하는 2007년 법률’이며, 주요 내용은 앞으로 5년 이내에 외국항만에서 미국행 화물에 대해 관련 시설을 갖추고 사전검색을 의무화해야 한다. 또한 항공의 경우는 3년 이내에 전면 시행하게 된다. 하지만 이 법률에 대해 백악관뿐만 아니라 해운업계, 무역업계, 그리고 국토안보부 등 관련 기관들도 반대하였다. 주요 이유는 현재의 국제 교역구조와 장비개발 수준을 고려할 때 100% 사전 검색은 실

제로 실행이 불가능하다는 것이다.

유럽연합은 이 제도가 시행될 경우 국제교역에 심각한 피해를 줄 것이라고 분석하였다. 컨테이너 화물의 100% 사전 검색은 화물을 검색하는 기술과 장비가 아직 충분히 개발되지 않은 상태이기 때문에 미국 수출 화물을 검색하는데 시간과 비용이 많아 소요되기 때문이다. 화물 검색 방법은 화물이 선적되기 전에 비파괴 영상장비와 방사능 탐지기를 사용해 2가지 검사, 즉 내장화물의 이미지 검색과 방사능 물질 탑재 여부탐지를 검사해야 한다. 우리나라의 경우 주요 항만에 설치되어 있는 화물 검색기는 밀수 방지를 위한 수입화물을 검색하는 데 사용되고 있어 새로운 검색기 설치가 불가피하다.

나. 검색 장비 현황 및 문제점

① 검색 장비

미국이 요구하는 컨테이너 내부 영상 검색과 방사능 탑재 여부를 동시에 검색하기 위해서는 처리 속도가 빠른 검사장비가 필요하다. 화물 검색기의 경우 SAIC (Science Application International Corporation)사와 SD(Smith Detection)사가 양분하고 있다. 최근 들어서는 중국의 누크테크(Nuctech) 사가 중국 정부의 적극적인 지원에 힘입어 동남아시아 등지에서 시장 점유율을 높여가고 있다.

i) SAIC사

현재 미국행 컨테이너 화물에 대한 100% 사전 검색 시범사업이 실시되는 부산 북항 감만부두 허치슨 터미널에 설치되는 장비는 미국 SAIC사의 제품으로 차량번호 인식기, 방사능 탐지기, X선 검사기 등의 기능을 수행하는 통합형 화물 검색기 SAIC P7500이다. 허치슨 터미널 게이트 4곳에 차량번호 인식기와 방사능 탐지기가 각각 설치된다. 그리고 X선 검사기는 게이트에서 120m 떨어진 곳에 고정식 게이트(높이 6m x 너비 8m) 형태로 설치된다. 차량이 X선 검색기를 통과하는 속도는 시속 8~13km로 알려지고 있으며, 이는 40피트 컨테이너 기준 시간 당 150개의 컨테이너를 검색할 수 있다. SAIC P7500 제품의 가격은 현재 1대당 25억으로 알려지고 있다. SAIC의 제품은 현재 미국의 동부지역 항만에서 사용되고 있으며, 이 회사는 자사 제품을 판매하기 위해 홍콩의 컨테이너터미널 운영사 협회와도 상담을 진행하고 있는 것으로 조사되었다.

<그림 5-6>

감마선을 이용한 이동식 검색기 VACIS



자료 : SAIC사

<그림 5-7>

X선을 이용한 고정식 검사기 SACIS P7500



자료 : SAIC사

ii) Smith Detection

Smith Detection사는 미국과 CSI 협정을 맺은 항만에 27개 시스템을 판매한 실적을 갖고 있다. 특히 공항에서의 화물 검색기를 전 세계에 판매하고 있다. 컨테이너 검사를 위한 고정식 검색기는 X선을 이용하여 시간당 25대의 트럭을 처리할 수 있고, 이동식 검색기는 1시간 이내에 설치 및 해체 가능하다고 이 회사는 밝히고 있다.

<그림 5-8>

X선을 이용한 고정식 검사기 HCVS

자료 : Smith Detection사

<그림 5-9>

X선을 이용한 이동식 검사기 HCV CAB 2000M

자료 : Smith Detection사

② 문제점

현재 컨테이너 화물 검색기에 사용되는 기술은 대부분 X-선을 이용하고 있어 검사 장비에 의한 방사선 피폭이 우려되고 있다는 점이다. 따라서 차량 기사들이 검색 자체를 거부할 가능성이 제기되고 있다. 그리고 100% 사전검색이 이뤄질 경우 검색하는 속도에 따라 화물 적체 문제가 발생할 가능성도 있다. 즉, 점차로 선박이 대형화되고 미국행 선박이 특정일에 기항하기 때문에 화물이 몰리고 일시에

화물의 검사가 이루어져야 하기 때문에 체증이 생길 수밖에 없다는 것이 업계의 주장이다.

③ 화물 검색기 부문 육성방안

현재 컨테이너 화물 검색기 시장에서는 SAIC사 또는 SM사의 제품을 사용하는 사례가 점차적으로 늘고 있다. 이들 회사가 미국에 기반을 두고 있고, 미국에서 컨테이너 화물 검색기 사용이 급증하고 있기 때문이다. 우리나라의 경우 밀수 화물 방지 차원에서 10대 이상의 컨테이너 화물 검색기를 주요 항만에 설치하고 있으나 이들 제품 중에 우리나라 기술로 개발된 검색기는 전무한 실정이다. 한 벤처 기업에서 고유 독자기술로 컨테이너 화물 검색기를 개발했으나 아직 상용화하지는 못한 것으로 알려졌다.

미국산 컨테이너 화물 검색기를 주로 사용하는 것은 미국의 보안기준에 따르는 것이 통관과정에서 유리할 것이라는 심중에 바탕을 두고 있는 것으로 보인다. 이와 관련해 미국은 조만간 컨테이너 화물 검색기에 대한 표준을 제정할 계획으로 있어 앞으로 미국산 검색기 사용이 더욱 늘어날 것으로 전망되고 있다. 따라서 미국이 일방적으로 제공하는 시스템보다는 터미널 사정과 터미널 운영에 적합한 장비가 도입되도록 국제적인 공조 체제를 형성할 필요가 있다. 그리고 우리나라의 경우 현재 부산항의 허치슨 터미널이 SAIC사의 제품을 설치하고 있는데, SAIC사 제품의 경우 X선 검색기에서 발생하는 방사선 피폭 때문에 미국 동부 항만의 차량 기사들이 검사기 통과를 기피한 사례가 발생되기도 하였다. 따라서 정부차원에서 이에 대한 피해 여부를 검토해야 한다.

현재의 검색장비와 기술 수준으로 볼 때 미국의 일방적인 화물의 100% 사전 검색이라는 물류보안 강화 조치는 물류 흐름의 혼란과 비용 부담으로 작용하고, 미국행 화물의 적체현상을 가중시키는 결과를 초래할 가능성이 크다. 현재로는 기술적으로 SAIC사의 제품의 경우 40피트 기준으로 시간당 150개의 컨테이너가 처리 가능하고, Smith Detection사의 경우 시간당 25대의 트럭이 처리 가능하다고 알려지고 있다. 이러한 기술적인 문제의 극복에는 시간이 소요될 것으로 판단되므로, 이에 대한 문제제기를 국제적인 차원에서 미국과 협의할 필요가 있다.

검사 장비 도입에 따른 비용 문제도 고려되어야 한다. SAIC사의 제품의 경우 1대당 25억원이 소요되며, 우리나라의 경우 약 400억 원으로 추정된다. 이는 터미널 운영비 증가에 따른 물류비 증가에 영향을 미치고 결국은 화주 및 소비자에게

이를 전가하는 상황이 발생할 소지가 높고, 이에 대한 정부의 대책이 필요하다. 이를 위해 정부는 보안 관련 장비 및 시스템의 도입에 따른 재정적 부담을 해소하기 위해 보안 할증료 제도를 정비하고 지원할 필요가 있다고 판단된다. 또한 우리나라에서 개발되고 있는 제품이 상용화되어 해외에 수출될 수 있도록 산업계 및 학계와의 연계를 강화하고 제품개발 자금 지원 및 민간자본 투자 중재 등을 고려할 필요가 있다. 중국의 경우 검색기 제조업체인 Nuctech사는 중국의 칭와대학교와 협력하여 선형입자가속기, 원자가속기, X선 분야 등의 기술을 집중 개발하고 있어, 우리나라도 고에너지 전자가속방출 기술, 고감도 X선 탐지기술, 이미지 프로세싱 등의 관련 기술에 대한 개발의 지원이 필요하다.

(3) 컨테이너 화물 추적 장치

가. 화물의 가시성에 대한 요구 증가

생산자에서 소비자에게 이어지는 물류 망을 실시간으로 완벽하게 통제할 수 있는 기술, 즉 ‘스마트 박스(smart container)’가 이용되고 있다. 이는 전자 태그(RFID)에 기반을 둔 화물추적 시스템으로서 기업이 생산한 제품이 컨테이너에 적입된 후 육상, 해상, 항공 등 운송수단에 의해 운송되고, 창고에 보관된 후 최종소비자에 이르는 전 물류구간을 추적·통제할 수 있는 시스템이다.

스마트 박스는 미 캘리포니아 주 오클랜드와 같은 주요 항구에서 무기 밀매와 같은 불법행위를 사전에 차단하기 위해 보안장치로 이미 활용되고 있는 기술이다. 스마트 박스는 아주 견고한 금속봉인(metal seal)에 고유번호가 매겨져 있고 자물쇠와 열쇠 뒤에 감지장치가 장착되어 세관원들은 박스 내부의 화물을 완벽하게 검사할 수 있도록 설계되어 있다. 기본 원리는 전자 태그를 이용해 컨테이너 안의 내용물을 체크하고, 수집된 정보를 소형컴퓨터로 전송하며, 소프트웨어가 GPS 수신기를 통해 현재의 위치를 파악한 뒤 정보를 결합한다. 이 박스에는 압력, 기온, 진동 등의 변수를 측정할 수 있는 다양한 센서가 통합되어 있어 무선 시스템을 통해 데이터베이스로 전송된다.

물류측면에서 이 시스템은 다양한 고객에게 인터넷을 통해 데이터베이스에 접속하여 상품의 현재 위치, 적합한 온도에서 운송되고 있는지 또한 운송도중 충격 등을 체크할 수 있다. 전자 태그 기술은 언제 어디에서 박스를 열 것인지 미리 지정할 수 있다. 박스에는 인증된 자동무선 카드의 전자 잠금장치 암호가 있어야만 열린다. 전자 태그에 기반을 둔 물류시스템을 통해 제조업체는 원자재의 흐름을

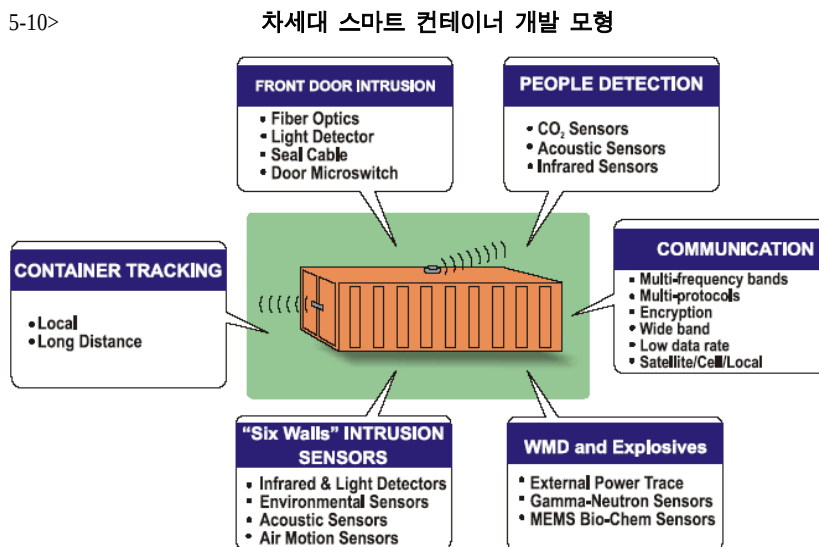
개선할 수 있으며, 판매자는 언제라도 필요한 곳에 상품을 배치할 수 있고 소매업자는 고객에게 원하는 제품을 정확하게 전달할 수 있다. 물류보안 측면에서는 2001년 9·11 테러 이후 각국의 물류보안조치를 강화하고 있어 물류 전 구간을 실시간으로 통제할 수 있는 시스템의 수요가 증가하고 있다. 특히 미국의 경우 반입되는 컨테이너에 대해 반강제적으로 RFID 태그를 부착하도록 하는 정책을 추진하고 있다. 연방통신위원회(FCC)의 웹 사이트에 따르면 미국은 2007년 4월에 반입되는 컨테이너에 RFID 태그를 부착하는데 필요한 규정을 개정하였다.

나. 스마트 컨테이너 장비 현황 및 문제점

① 장비 현황

Smart Container를 생산하고 있는 기업은 세계적으로 약 31개사로, 69개의 제품을 출시하고 있는 것으로 알려지고 있다. 향후 Smart Container 기술 개발은 컨테이너의 개폐여부를 감지하기 위해 광학섬유, 광선, 날인 케이블, 자동제어의 고감도 스위치 등을 적용한 기술이 개발될 것으로 예상된다. 사람의 탑승 유무를 검사하고자 이산화탄소 센서, 음향 센서, 적외선 센서 등의 기술이 사용되며, 대량살상무기를 감지하기 위한 감마-중성자 센서, 지능형 바이오-화학무기 센서 등도 사용될 것으로 예상된다.

<그림 5-10>



자료 : 미국 국토안보부 연구소

② 문제점

스마트 컨테이너는 정보통신산업과 결합된 차세대 최첨단 화물 운송용기이다. 이 같은 개념에 따라 현재 세계적으로 유비 쿼터스 정보화 시대의 주요 기술인 RFID/USN과 결합된 스마트 컨테이너에 대한 관심이 집중되고 있다. RFID/USN은 기본적으로 3가지 구성 요소로 구성되어 있는데, 즉 사물의 식별 정보를 저장하는 태그, 태그를 판독하는 리더기, 그리고 서버 및 미들웨어, 응용프로그램으로 구성된 애플리케이션이다. 미국의 경우 MIT를 중심으로 북미 지역 코드관리기관(UCC : Uniform Code Council), 국방성, 민간 업계 등과 협력해 'Auto-ID 센터'를 1998년에 설립해 기술 개발 및 상용화를 추진하고 있다. 유럽은 2001년부터 정보화사회 기술계획(IST)의 일환으로 'Disposing Computing Initiative' 사업을 통해 관련 기술을 개발하고 있다. 그리고 일본은 국가의 유비 쿼터스 컴퓨팅 환경을 구축하고자 '유비 쿼터스 ID 센터'를 2005년 설립하였다. 우리나라의 경우 센싱형 RFID는 2007년까지, USN은 2010년까지 핵심 기술 및 시스템을 개발할 계획이다.

Smart Container도 RFID/USN 기술을 응용하여 물류에 적용된 시스템으로서 향후 그 시장성은 매우 크다. 그러나 우리나라는 요소 기술 개발과 더불어 제품에 적용하는 비즈니스 모델의 개발이 미흡한 것으로 판단된다. 현재 우리나라는 이에 대한 제품을 생산하는 기업은 없는 것으로 조사되었다. 그러나 IBM사는 컨테이너 해상운송 업체인 머스크 로지스틱스와 협력해 컨테이너 보안과 위치정보를 추적하는 보안 장비를 개발했다고 2005년 9월 17일 발표하였다. IBM사가 개발한 시스템의 주요 구성요소는 컨테이너 도어에 부착된 부정 개폐방지 장치와 습도와 온도 등을 감지하는 센서, 그리고 위치정보를 추적하는 GPS이다. 이 회사는 뉴욕에서 열린 해양보안 엑스포 및 학회에서 무선방식을 사용한 자사의 제품이 타 제품과 차별화되었으며, 무선방식을 이용해 화물의 상태를 실시간으로 추적함으로써 재고 수준을 낮추고, 비용 절감을 할 수 있는 장점이 있다고 주장하였다.

다. 스마트 컨테이너 부문 육성방안

현재는 해외에서만 다수의 업체가 다양한 형태의 Smart Container를 출시하고 있다. 그러나 우리나라의 경우 Smart Container에 적용할 수 있는 세부 기술의 개발이 진행되고 있으나 아직 상용화하지는 못하고 있다. 다만, 2005년 1월 9일 정보통신부와 산업자원부는 RFID(Radio Frequency IDentification) 분야에서 부처간 공조 체계를 구축하면서 RFID 사업의 활성화를 추진하고 있다. 또한 우리나라는 전자상

거래표준화통합포럼(ECIF)을 중심으로 진행되고 있는 RFID 관련 기관의 표준화 협력에 각 유관기관의 적극적인 참여를 유도하고, 민간차원에서 차세대 RFID 기술과 서비스의 개발이 효율적으로 이루어지도록 기술 개발의 방향 및 내용을 제시 하기도 하고 있어 기술을 확보하는 데는 큰 문제가 없다는 판단이다.

우리나라는 전 세계 Smart Container 시장이 40억 달러 규모인 것을 감안할 때 이에 대한 비즈니스 모델의 개발에 관심을 가져야 한다. Smart Container의 경우 물류보안의 문제뿐만 아니라 컨테이너 화물정보를 관리하면서 생산자에서 소비자에 이르는 전 물류구간의 화물을 실시간으로 추적하고 통제를 해결할 수 있는 시스템이다. 현재 전자 봉인 시스템의 개발과 보급을 주도하고 있는 Savi Technology나 GE사 등이 기존의 자사 시스템을 활용하여 Smart Container 시장으로 사업 영역을 확대할 것은 분명한 사실이다. 이는 국내 Smart Container 기술의 부재로 기술 종속 뿐만 아니라 물류 정보에 대한 통제권을 상실하는 경우도 발생할 수 있다. 따라서 우리나라도 국가적인 차원에서 Smart Container에 관련된 기술개발과 향후 화물 정보관리에 대한 국가적인 차원의 관리방안이 수립되어야 한다.

이를 위해 정부는 Smart Container와 관련된 기술을 개발하고 있는 산업계와 연계하여 우리나라의 성장 동력산업으로 채택하고, 세제 혜택이나 연구개발의 적합성을 판단하여 자금지원, 파이낸싱 등의 재정적 지원이 가능하도록 하는 제도적 장치가 필요하다고 판단된다.

(4) 물류보안 기술개발 연구사업

가. 현황과 필요성

물류보안 분야의 기술개발 사업이 시급하다. 현재 물류보안 분야의 기술은 대부분 특허로 등록되거나 외국업체가 독점을 하고 있어 기술종속이 우려되는 수준이다. 특히 컨테이너 화물 보안장치에 대한 원천기술 미확보 문제도 해결해야 할 난제다. 컨테이너 봉인장치(E-seal) 등 보안장비 표준여부에 따라 기술종속이 고착화될 개연성이 커지고 있기 때문이다.

이에 따라 스마트 컨테이너 개발 조기 착수가 대안으로 떠오르고 있다. 우리나라가 미래 컨테이너 보안장비 시장에서 주도권을 확보하기 위해선 ‘스마트 컨테이너’ 개발에 대한 투자가 조기에 집행돼야 한다는 것이다. 블루오션을 미리 개척해서 국제표준을 확보할 경우, 시장창출은 물론 기존 보안장비 원천기술 보유회사와의 특허 협상에서도 유리한 고지를 점령할 수 있기 때문이다.

그리고 2012년 시행 예정인 100% X-레이 사전검색과 관련하여 국산화가 필요한 핵심 장비개발에 대한 정책적 예산지원도 면밀히 검토되어야 할 단계다. 컨테이너 내부 영상검색과 방사능 물질 탑재 여부를 동시에 검색하기 위해선 미국의 사비 등 고가 장비가 필요하기 때문이다. 현재 상용화되고 있는 컨테이너 화물 검색기는 시간당 30TEU 안팎의 컨테이너를 처리하고 있다. 이에 따라 향후 부산항 등 국내 터미널에 필요한 검색기만도 수십 대에 이를 전망이다. 시장도 1,000억원 이상에 달할 전망이다.

그러나 물류보안 기술개발에 참가하는 업체는 극히 일부에 불과하다. 물류보안 분야가 최근에 생성된 개념이고 급격히 제도화되었기 때문이다. 특히 보안산업의 특성상 일부 업체에 의해 기술이 독점되고 있어 후발주자들의 시장 참여가 쉽지 않다.

나. 정책과제

정부는 물류보안기술개발 및 연구개발 업체 양성을 위한 적극적 지원책을 마련해야 한다. 첫째, 물류보안산업 육성을 위한 기본계획을 마련하고 연구기술개발을 위한 세부전략을 포함해야 한다. 이를 위해 정부에서 기술개발 장기계획을 마련하고 민간 사업자가 참여할 수 있도록 해야 한다.

둘째, 물류보안기술개발 업체에 대한 지원책 마련이다. 이를 위해 물류보안기술개발분야에 ‘성공불 용자’ 도입을 제안한다. 성공불 용자란 대규모 투자가 필요하나 투자금 회수 기간이 길고 리스크는 높은 사업에 대해 자금을 빌려준 뒤, 성공하면 원리금에다 특별 부담금까지 받지만 실패할 경우에는 원리금 상환부담을 대폭 경감해 주는 제도다. 현재 유전 개발 등 해외자원개발사업 등에 쓰이고 있다. 물류보안 기술을 개발하는 데는 자금부담과 리스크가 크기 때문에 국내 물류보안업체의 참가가 쉽지 않으나 경제 및 물류기술의 대외종속을 막기 위해서는 필요한 상황이다.

(5) 물류보안교육 및 컨설팅 부문

가. 현황과 필요성

물류보안산업의 확산과 육성을 위해 요구되는 또 다른 분야는 물류보안교육 및 컨설팅 부문이다. 물류보안제도를 수용하지 않을 경우 제조업체 및 무역업체의 미국 등 해외수출이 불가능해질 수 있기 때문이다.

현재 물류보안제도는 미국에 의해 주도되고 국제기구에서 수용하면서 확산되고 있다. 문제는 물류보안제도를 수용하지 않을 경우 일반 제조업을 비롯한 무역

업체들의 미국 등 해외 수출이 어렵게 된다는 점이다. 우리나라는 일찍부터 수출 의존형 경제구조를 가지고 있고 대부분의 기업은 내수 판매와 더불어 수출을 중요한 성장전략으로 활용하고 있다. 물류보안제도는 제품의 생산지와 상관없이 도착지가 미국 또는 ‘미국식’ 물류보안제도를 수용하는 국가에서는 수용해야 한다. 우리나라 기업의 중국 현지 생산도 미국으로 수출하기 위해서는 물류보안제도를 수용해야 한다는 뜻이다.

따라서 향후에는 물류보안교육과 컨설팅 수요가 다양하게 발생할 것으로 예상된다. 물류보안교육은 일차적으로 물류보안에 종사하는 임직원이 대상이 되고, 그 다음은 물류업체 임직원, 그리고 수출업체 직원으로 확산될 것이다. 물류보안의 교육 내용은 물류흐름, 물류보안제도, 물류보안확보방안, 물류보안시스템구축, 물류보안사고시 대책 등이 포함될 것이다. 물류 컨설팅은 업체에서의 물류보안시스템 구축방안, 물류보안인증방안, 물류보안시스템 관리 효율화 방안, 물류보안비용 절감 방안 등이 주요 내용이 될 것이다.

현재 물류분야의 컨설팅은 주로 IT 분야와 물류시스템 개선분야에 집중되고 있다. 그러나 IT 업체의 물류분야 매출은 매우 낮은 것으로 파악되고 있다. 더구나 물류보안만 전문으로 하는 컨설팅 업체는 없는 것으로 파악된다. 아직 물류보안 컨설팅 시장이 형성되지 않았기 때문이다.

<표 5-8>

국내 물류관련 IT 업계의 물류분야 매출 비중

단위 : 억원

구분	매출 (2006년)	물류 IT 매출비중
동부정보기술	1,550	5~6%
신세계아이앤씨	2,005	1~2%
아시아나 IT	1,400	4~5%
한진정보통신	850	5~6%
CJ 시스템즈	1,508	8~9%
KE 정보기술대한통운	260	63%

자료 : 「월간 경영과 컴퓨터」, 2007년 5월.

이런 상황은 다음과 같은 지적에서 잘 나타난다. “단적으로 많은 기업들이 아직 까지 보안업무의 중요성을 깨닫지 못하고 있다고 할 수 있다. 뿐만 아니라 보호해

야 될 중요한 정보가 무엇인지에 대한 구분도 못하고 있는 실정이다. 이런 국내 기업들을 돕기 위해 보안체계를 점검하고 취약점을 진단해 문제점을 해결해주는 보안 컨설팅 업체가 필요하다.”⁹⁶⁾

나. 정책과제

물류보안교육 및 컨설팅 부문의 지원방안으로 구상할 수 있는 내용은 다음과 같다. 첫째, 물류보안교육 프로그램 개발 및 지원이다. 현재 국내에는 물류보안을 교육할 수 있는 시설, 전문기관, 교육 프로그램이 구비되지 않았다. 현재 물류보안 인력에 대한 교육도 경비업체를 대상으로 하는 교육이 대부분을 차지한다. 따라서 대학이나 연구소에서 물류보안교육 프로그램을 개발하고 이를 교육할 수 있도록 해야 한다.

둘째, 물류보안교육에 대한 교육비 지원이다. 이를 위해서는 고용보험의 직업능력개발사업 대상에 물류보안교육을 포함하여 교육비의 일부를 지원할 수 있도록 해야 한다.

셋째, 물류보안 컨설팅 업체에 대한 지원이다. 물류보안업체에 대해 물류업체와 같은 지원책을 마련해야 한다.

96) 자료 : Security World.

제6장 결론 및 정책 제언

1. 연구 결론

1) 물류보안은 글로벌 메가 트렌드

물류보안이 글로벌 메가 트렌드(global mega trend)로 자리 잡고 있다. 2001 9·11 항공기 테러 이후 주요국들이 물류보안조치를 크게 강화하고 있기 때문이다. 특히 이 같은 경향은 미국을 중심으로 국제사회로 더욱 확산되고 있다. 미국의 경우 2003년과 2006년에 해운 보안법과 항만 보안법을 제정한 이후 최근에는 9·11 테러 대책 이행법률을 제정하면서 자국으로 수출되는 모든 컨테이너 화물을 100% 검색하는 제도를 도입하였다. 유럽연합 또한 기존의 물류보안제도를 강화하면서 기업 물류보안 인증제도(AEO)를 도입, 2008년부터 본격적으로 시행할 예정이다. 싱가포르의 아시아권에서는 처음으로 2007년 5월에 ‘안전한 교역 프로그램(STP)’을 도입, 발 빠르게 물류보안제도 확산에 대응하고 있다. 이에 그치지 않고, 뉴질랜드도 세계세관기구의 SAFE Framework를 기초로 미국과 물류보안 협정을 체결했으며, 중국은 유럽연합과 미국의 항만을 대상으로 컨테이너 화물추적 시범사업에 착수하였다. IMO와 WCO, 그리고 국제표준기구(ISO) 등 국제기구에서도 물류보안제도 정착에 적극 나서고 있다.

2) 주요국, 물류보안제도 더욱 강화

이와 같이 물류보안제도가 세계교역질서의 새로운 패러다임으로 자리 잡고 있는 가운데, 9·11 테러 이후 다양한 물류보안제도를 도입한 국가들은 기존의 제도를 더욱 강화하는 경향을 보이고 있다. 전문가들은 물류보안이 글로벌 메가 트렌드로 정착됨에 따라 앞으로 이 같은 추세가 더욱 강화될 것으로 전망하고 있다.

(1) 선박과 항만 보안제도 확대

9·11 테러 이후 선박과 항만시설의 보안을 강화하기 위해 도입된 IMO의 ISPS 코드 등도 강화되고 있다. IMO는 ISPS 코드를 개정해 2008년부터 선박에 장거리

선박 위치추적 시스템 설치를 의무화하는 한편, 이 코드의 적용대상에서 벗어나 있는 500톤 이하 선박까지 적용을 확대하는 방안을 검토하고 있다. IMO는 2007년 10월 2일부터 코펜하겐에서 개최된 해상안전위원회(MSC)에서 이 문제를 심도 있게 논의하고 있다. 이에 앞서 IMO는 이 문제를 다룰 특별 위원회를 MSC 산하에 설치하고, 필요한 준비작업을 진행하라고 지침을 준 바 있다. IMO는 또한 물류보안업무에 종사하는 선원 등이 적절한 교육·훈련은 물론 자격증을 취득하는데 도움을 주기 위한 회람문서를 마련, 회원국에 제공하기로 하였다. 미국은 2003년에 제정된 해운보안법에 따라 외국 항만의 보안위협에 대한 평가를 지속적으로 수행하는 한편, 2007년 10월 1일부터는 단계적으로 200만 운수근로자를 대상으로 신분증을 발급하는 작업에 착수하였다. 운수근무자 신분증 발급제도는 신원조사(background check)와 지문을 확보하는 것이 주목적인데, 미국은 이 제도 시행과 함께 중요한 범죄를 범한 자에 대해서는 항만 등에 취업을 금지하는 방안도 마련한 바 있다.

(2) 항만서 컨테이너 검색 강화

컨테이너 화물에 대한 검색제도도 강화되고 있다. 2006년 기준으로 전 세계 항만에서 처리된 컨테이너 물동량은 4억 4,190만TEU이며, 이 중 북미 지역 물동량은 4,800만TEU에 달하였다. 미국은 이 같은 컨테이너 화물을 통해 대량살상무기(WMD) 등 자국의 안보를 저해하는 위험물질이 몰래 반입되는 것을 사전에 차단하기 위해 2002년에 이른바 컨테이너보안협정(CSI)을 도입하였다.⁹⁷⁾ 이 협정에 따라 현재 전 세계 54개 주요 항만에서 미국행 컨테이너 화물에 대한 검색활동이 이뤄지고 있다. 미국의 컨테이너 화물 사전 검색제도는 화물 통관과 관련한 기존의 관행을 송두리째 변화시켰다는 점에서 국제교역에서 새로운 패러다임으로 인식되고 있다. 즉, 지금까지 수입되는 화물에 대한 검사는 자국 항만에 양륙된 뒤 실시하는 것이 일반적이었으나 컨테이너 화물검색제도에서는 외국항만에서 선박에 화물이 선적되기 전에 실시되고, 그 화물에 대한 정보도 사전에 제공하도록 되어 있기 때문이다.

한편, 미국은 이 같은 제도 시행과는 별도로 2006년 8월에 항만보안법을 제정해 우리나라의 부산항 허치슨 감만 터미널을 포함해 세계 7개 항만에서 컨테이너 화

97) 미국의 세관·국경보호청(CBP)이 2002년에 CSI를 도입한 이후 에너지부는 MI(대형항만 방사능 탐지 제도)를 도입, 컨테이너 화물의 방사능 탐지 기능을 확대하였음.

물 100% 검색 시범사업을 단계적으로 진행하고 있다. 그리고 2007년 8월 3일에 외국항만에서 컨테이너 화물의 100% 검색을 의무화하는 9·11 테러 대책 이행 법률을 제정하였다. 9·11 테러 이후 5년 동안 미국은 자국으로 들어오는 컨테이너 화물에 대한 검색 비율을 새로운 입법을 통해 2% 수준에서 100%까지 높이는 한편, 검색 방법도 양자협정에 기반을 두고 이뤄지던 것에서 미국의 일방적인 입법으로 선화하였다.

3) 물류보안 인증제도 시행 확산

9·11 테러 이후 물류보안 인증제도도 널리 확산되고 있다. 물류보안 인증제도는 국제 교역에 참여하는 기업이 보안 기준을 충족하고 있는지 여부를 심사한 후 일정한 자격을 부여하는 것을 말한다. 일반적으로 정부 등에서 물류보안 인증을 받은 기업은 수출입 화물을 통관하는 과정에서 검사를 간소화하는 등 일정한 혜택을 부여받게 된다.

본래 이 제도는 미국의 C-T PAT에서 처음 출발한 뒤 WCO를 거쳐 글로벌 기준으로 정착되어 확산되고 있다. 미국의 경우 2006년 12월 기준으로 C-T PAT에 따라 인증을 받기 위해 신청서를 제출한 기업이 1만 4,000개를 넘는 것으로 나타났다. 미국은 당초 예상보다 가입 희망자가 폭증함에 따라 이 업무를 전담하는 인터넷 포털 사이트를 개설하는 한편, 물류보안 인증 심사관을 해마다 50명 정도 증원한다는 계획도 세워 놓고 있다. 또 미국은 중국 등 자국 심사관을 파견하기가 곤란한 나라에서 물류보안 심사업무를 담당할 민간 인증심사기관을 별도로 지정하여 운영하고 있다.

한편, 2005년 8월에 WCO가 미국의 C-T PAT과 CSI의 주요 내용을 통합한 SAFE Framework를 채택한 이후 이 제도를 도입하는 나라도 늘어나고 있다. 유럽연합의 경우 WCO에 기반을 둔 물류보안 인증 사업자제도(AEO)를 입법화하고, 2009년부터 본격적으로 시행할 예정이다. 싱가포르와 뉴질랜드 등도 이 같은 대열에 동참하고 있다. 싱가포르의 경우 안전한 교역 프로그램(STP)을 제정하고, 국제 교역에 종사하는 화주를 대상으로 물류보안 인증제도를 2007년 5월부터 시행하고 있다.

일본은 지난 2월 관세법을 개정하고, 수출입 화주를 대상으로 물류보안 인증사업에 착수한 데 이어 국토교통성도 운송기업에 대한 인증제도 도입을 2007년 안에 도입한다는 방침이다. 특히 일본과 싱가포르 등은 자국의 기준에 따라 물류보안

인증을 받은 기업이 다른 나라에서도 동일한 자격과 혜택을 부여 받을 수 있도록 미국 등과 물류보안 상호 인정협정을 체결하는 방안을 추진하고 있다. 중국과 베트남도 2007년 안에 물류보안 인증제도를 도입한다는 계획에 따라 필요한 절차를 진행하고 있다. 우리나라도 관세청이 관세법 개정안을 마련함으로써 이 제도를 도입하기 위한 절차에 돌입하였다.

4) 글로벌 물류보안 정보 과점화

물류보안 정보를 획득하거나 확보하기 위한 움직임도 빨라지고 있다. 미국이 2002년에 CSI 제도를 도입한 것과 때를 맞춰 시행하기 시작한 이른바 ‘24시간 규칙’이 새로운 형태로 진화하고 있다. 24시간 규칙은 컨테이너 화물 정보(적화목록, manifest)를 선박에 선적하기 24시간 전에 미국 세관·국경보호청에 신고, 제출하도록 하는 제도이다. 미국은 사전에 제출된 정보를 토대로 자국에 반입되는 컨테이너 화물의 위험성 여부를 판단하는 근거로 활용하고 있다. 또한 CSI를 시행하고 있는 항만에도 컨테이너 화물에 대한 정보를 제공, 정밀 검색활동에 활용하고 있다.

이 제도와 관련하여 미국은 현재 두 가지 새로운 제도를 추진하고 있다.

첫째, 보다 엄격한 위험화물 차단을 위해 기존 제도를 보완하는 ‘10+2 규칙’을 2008년 1월부터 시행할 방침이다. 지난 2007년 9월 관세·국경보호청이 밝힌 바에 따르면, 미국은 내년 1월부터 화주에 대해서는 10개 항목의 자료를, 그리고 선사에 대해서는 2개 자료를 추가적으로 제출하도록 할 계획이다. 특히 미국이 입법을 추진하고 있는 ‘10+2 규칙’은 미국으로 수출하는 화물의 모든 정보를 요구하고, 선사에 대해서는 선박 적재계획까지 제출하도록 하는 내용을 담고 있어 현재 제조기업 및 해운회사들의 상당한 비판을 받고 있다. 이 제도가 시행되면 사실상 기업의 거래정보까지 미국에 넘어가는 결과를 초래할 수 있기 때문이다.

둘째, 여기에 덧붙여 미국은 ‘글로벌 트레이드 익스체인지(Global Trade Exchange)’라는 거대한 물류보안 데이터베이스를 구축하는 사업에 착수하였다. 자국에 모아진 기업 및 화물 정보뿐만 아니라 컨테이너 화물 검색 등을 통해 확보한 물류보안 정보를 통합, 공유한다는 것이 미국의 계획이다.

한편, 미국의 이 같은 물류보안 통합화·독점화 작업과는 별도로 글로벌 컨테이너 전자 봉인 및 추적 시스템 시장을 양분하고 있는 GE 그룹과 사비 테크놀로지

등도 물류보안 정보를 선점, 상품화하는 전략을 추진하고 있다. 이들 기업은 전자 태그와 컨테이너 전자 봉인 시스템을 운영하는 과정에서 획득하는 정보를 자체적으로 구축한 글로벌 데이터베이스에 축적, 필요로 하는 기업에 제공하는 비즈니스 모델을 추진하고 있다.

5) 물류보안산업, 새로운 수익모델

물류보안이 글로벌 스탠더드로 자리 잡으면서 물류보안산업도 새로운 시장으로 성장하고 있다. 아직 시장이 형성되는 초기이기 때문에 현재 상태에서 물류보안산업을 정확하게 평가하기에는 한계가 있다. 그러나 국제적으로 강화되고 있는 물류보안제도를 시행하는데 필요한 각종 장비 및 기술, 시스템, 소프트웨어, 그리고 컨설팅 분야의 업무를 모두 망라하는 경우 물류보안산업의 규모는 상당히 확대된다.

특히 미국이 최근에 9·11 테러 대책 이행법률을 제정하면서 항공 및 해상 컨테이너 화물에 대해 100% 사전 검색을 의무화하는 한편, 도로 및 철도부문의 보안을 더욱 강화하고 나섬에 따라 앞으로 시장 규모는 더욱 크게 확대될 것으로 보인다.

우리 원이 조사한 자료에 따르면, 컨테이너 보안 장비(CSD) 및 검색, 전자 태그(RFID) 시장은 2010년에 90억 달러에 이를 전망이다. 이에 따라 GE나 록히드 마틴 등 글로벌 기업의 물류보안 시장 참여도 본격화되고 있는 것으로 나타났다. 즉, 현재 물류보안산업과 관련하여 시장 규모가 가장 큰 것으로 평가되고 있는 컨테이너 보안 장치(CSD) 및 전자 태그·컨테이너 전자 봉인 시장은 GE와 록히드 마틴이 각축전을 벌이고 있는 실정이다. 또한 컨테이너 화물 검색기 시장은 스미스 디텍션, 중국의 누크테크, 미국의 SAIC 등 3파전을 형성하고 있다. 특히 미국이 2012년부터 컨테이너 화물에 대한 100% 검색을 의무화하고, 전자 봉인 등에 대한 표준을 제정하기로 함에 따라 신속하게 화물을 검색할 수 있는 OCR 및 방사능 탐지기, 화물 검색기 기능이 통합된 모델이 더욱 각광을 받을 가능성이 큰 것으로 판단된다.

6) 우리나라 물류보안은 ‘중간단계’

이 같은 국제적인 추세와 여러 가지 여건에 견줘봤을 때 우리나라의 물류보안 수준은 어느 정도인가? 보는 시각에 따라 다양한 평가가 나올 수 있으나 준비단계

를 조금 지난 중간 수준에 이른 것으로 보는 것이 일반적이다. 우선 물류보안을 확보하기 위한 최소한의 법적 기반이 구비되어 있고, 현재 지속적으로 입법 작업을 진행하고 있기 때문이다. 단순히 제도적인 여건을 봤을 때는 대강의 입법 작업은 이뤄진 것으로 평가된다. 예컨대 항공부문의 경우 9·11 테러 이전에 이미 항공안전 및 보안에 관한 법률이 제정되어 시행되고 있고, 해운물류부문에서는 2007년 5월에 ISPS 코드를 수용한 국제 항해선박 및 항만시설의 보안에 관한 법률이 마련되었다. 또한 최근 관세청은 관세법을 개정해 물류보안 인증제도(AEO 제도)를 도입하기 위한 절차에 들어갔다.

다만, 문제는 이 같은 입법 추진에도 불구하고, 아직까지 우리나라에서는 물류보안에 관한 정부기관의 업무 추진동력이 힘을 받지 못하고 있을 뿐만 아니라 종합적인 관점에서 물류보안을 확보하기 위한 정책 대안이 마련되어 있지 않다는 점이다. 즉, 통합적인 관점에서 물류보안을 시행하기 위한 계획이 없고, 정부 각 부처가 산발적으로 제도를 도입·운영하고 있다는 점이다.

또한 민간부문과 정부 부문의 물류보안에 대한 인식의 차도 현격한 것으로 드러나고 있다. 특히 민간부문의 경우 제도 성격상 물류보안을 부담요인이나 하나의 규제조치로 받아들이는 경향이 강한 것이 현실이다. 이는 물류보안제도가 도입되는 경우 비용 지출이 늘어나고, 화물의 원활한 흐름을 저해할 것이라는 현실적인 우려에 뿌리를 두고 있다. 따라서 앞으로 우리나라가 국제적인 기준에 맞는 물류보안제도를 도입하는 경우에는 민간의 부담을 줄일 수 있는 인센티브나 부담을 완화할 수 있는 대안이 있어야 한다는 점을 의미한다.

이에 덧붙여 우리나라의 경우 국제적으로 강화되고 있는 물류보안제도를 활용하기 위한 정부 및 민간 부문의 정책 솔루션이나 비즈니스 모델이 개발되어 있지 않은 실정이다. 이 같은 모습은 물류보안제도를 성장의 발판으로 삼고 있는 싱가포르나 홍콩의 전략과 크게 다른 점이다. 세계 최대의 환적 항만으로 성장한 싱가포르의 경우 9·11 테러 이후 적극적으로 물류보안제도를 도입, 자국의 물류경쟁력을 제고하고 있는 대표적인 나라이다. 홍콩 또한 이와 크게 다르지 않다.

민간 기업 또한 물류보안에 실질적으로 필요로 하는 다양한 보안기술 및 장비, 시스템 등을 개발하는 등 물류보안 시장에 적극 참여하고 있다. 이에 비해 우리나라 기업의 경우 전자 태그나 컨테이너 화물 검색기 사업 등에 발을 내밀고 있으나 세계 시장을 장악하고 있는 글로벌 대형 기업과 경쟁하기에는 아직 힘이 부친다는 것이 업계와 전문가들의 객관적인 평가이다.

2. 정책 제언

물류보안은 현실적인 요청이다. 우리나라의 경우 항만을 포함한 일부 시설물에 대해서는 ‘적의 침입에 대비하기 위한 보안’이 상당부분 확보되어 있다. 과거 냉전 시대 남과 북이 치열하게 대치하고 있던 상황에서 국가 중요 시설물을 보호할 필요성이 강력하게 요청되었기 때문이다. 그러나 최근의 물류보안제도는 9·11 테러라는 외생적인 변수에 의해 강화되고 있다는 점에 유의할 필요가 있다. 그 기준도 과거 우리나라의 보안규정에 따르는 것이 아니라 글로벌 스탠더드로 정립되고 있다. 현재의 물류보안은 로 컨테이너 화물이 국제적으로 운송되는 과정에서 발생할 수 있는 테러를 차단하는데 목표를 두고 있기 때문이다.

이에 따라 앞으로 컨테이너 화물 검색, 컨테이너 전자봉인 장치 사용, 컨테이너 화물 추적 및 물류보안 정보 시스템 구축, 물류보안 인증제도 등을 수용할 수 있는 제도적·기술적 기반을 마련하는 것이 시급한 과제로 등장하였다. 앞으로 우리나라의 물류보안제도는 기존의 제도에 기반을 두되, 새로운 시대사조에 따라 과감하게 변모시킬 필요가 있다. 앞에서 언급한 연구 결론을 토대로 우리나라가 국제기준에 맞는 물류보안제도를 정립하고, 국가 물류 경쟁력을 확보하기 위해서는 다음과 같은 부문에 정책적 역량을 강화해야 할 것으로 분석되었다.

1) 국가 물류보안계획 수립·시행

2001년 9·11 테러 이후 글로벌 물류보안제도는 미국이 선도하고, 국제기구가 추종하는 형태로 추진되면서 하나의 글로벌 기준으로 정착되고 있다. 이 제도가 처음 도입될 당시에는 항만이나 선박 등 극히 일부 구간의 보안을 확보하는데 초점을 두고 있었다. 그러나 2005년 WCO에서 SAFE Framework를 제정한 것을 계기로 글로벌 물류보안제도는 물류 전 구간의 보안을 확보하는 이른바 통합 물류보안이 대세를 이루고 있다. 즉, 물류 각 결절(node)마다 부분적·단편적으로 시행하던 물류보안제도를 통합적인 관점에서 재구성하고, 흠결이 드러난 부문을 보완함으로써 글로벌 물류보안제도가 완성되고 있다.

따라서 우리나라도 이 같은 세계적인 추세를 반영하여 기존 보안제도를 토대로 국제기준에 맞는 새로운 물류보안제도를 도입할 필요가 있다. 문제는 이 같은 국제적인 추세를 반영할 수 있는 시스템이 갖춰져 있지 않다는 점이다. 현실이 이렇

다보니 각 정부 부처는 전체적인 측면에서 우리나라 물류보안업무를 통합 조정할 기능 및 계획이 없다는 것이 문제점으로 지적되고 있다. 특히 현재 국제적으로 시행되고 있는 물류보안은 컨테이너 화물을 중심으로 진행되고 있어 화물의 제조에서 최종 소비에 이르기까지 완벽한 보안 시스템 구축을 전제로 하고 있다. 다시 말한다면, 이 같은 물류 흐름에는 다수의 정부 부처가 관련되어 있어 하나의 계획에 따라 물류보안 업무의 통합과 시행이 필요하다.

이에 대한 대안으로 이 연구에서는 가장 ‘국가 물류보안 계획’을 수립·시행할 것을 제안하고자 한다. 즉, 현재 정부 각 부처간에 분산되어 있는 물류보안업무를 하나의 국가계획으로 수립한 다음, 통합적인 관점에서 우리나라 물류보안제도를 시행하는 것이 업무 추진상의 시너지 효과를 제고할 수 있을 것으로 판단되기 때문이다.

국가 물류보안 계획을 수립하는 근거는 2007년 7월에 국회에서 통과된 물류정책기본법⁹⁸⁾에 따라 수립하게 되어 있는 국가물류기본계획을 활용하면 큰 문제가 없을 것으로 분석된다. 물류보안도 광의로는 물류정책에 포함되는 것이므로 이 같은 대안을 선택하는 것이 이상적인 것으로 판단된다. 특히 국가물류기본계획을 최종적으로 심의·확정하는 기관이 국무총리를 위원장으로 하는 국가물류정책위원회로 격상되어 이 안을 택할 경우 관련 부처 간에 분산되어 있는 물류보안 업무를 효율적으로 통합·조정하는데 적합하다는 의견이다.

한편, 국가 물류보안 계획에는 1) 우리나라 물류보안에 관한 기본 방침과 2) 중장기 정책방향을 정하고, 3) 각 부처별 국가 물류보안체제 구축에 관한 사항을 정한다. 이와 함께 이 계획에는 4) 물류보안 인프라 구축에 관한 사항, 5) 물류보안 전문인력 양성, 6) 물류보안 연구개발 추진 및 7) 물류보안산업 육성 및 지원에 관한 사항, 8) 테러 사태 발생에 따른 신속한 대응방안, 그리고 9) 물류보안에 관한 국제협력 등을 반영하면 크게 무리가 없을 것으로 보인다.

2) 물류보안 관련 법률의 개선

주지하는 바와 같이 우리나라의 경우 현재 물류보안과 관련하여 두 가지 법률이 제정되어 시행되고 있다. 9·11 테러 이전부터 도입한 항공안전 및 보안에 관한 법률과 2007년 5월에 제정한 국제선박 및 항만시설 보안에 관한 법률이 그것이

98) 이 법률은 2007년 8월 3일 공포되어 2008년 2월 3일부터 시행될 예정이다.

다. 전자는 주로 항공운송부문의 안전과 보안을 확보하기 위한 법률인 반면에 후자는 9·11 테러 이후 국제해사기구(IMO)에서 제정한 이른바 ISPS 코드를 우리나라에서 수용하기 위해 입법한 것이다. 이 법률이 제정되기 전에 우리나라는 고시를 제정하여 ISPS 코드를 시행해 왔다. 고시와 법률에 담겨 있는 내용 가운데 가장 큰 차이점은, 고시에는 없는 국가항만보안계획의 수립 및 시행, 항만시설 보안료의 부과·징수, 그리고 법률의 강행규정을 위반한 경우의 처벌 규정 등이 법률에는 반영되어 있다는 점이다.

문제는 이와 같이 항공과 해운 및 항만부문을 포괄하는 두개의 법률이 있음에도 불구하고, 우리나라의 경우 글로벌 물류보안제도를 제대로 시행하는 데 한계가 있다는 점이다. 즉, 기존의 법률은 각각 ICAO와 IMO 등에서 도입한 부문별 보안제도를 시행하기 위해 제정되었다. 이에 따라 화물의 자연스런 이동을 보장하면서 통합적인 관점에서 물류 전구간의 보안을 통합하고, 조정할 수 없다는 난점이 있다. 또한 정부 각 부처에서 물류보안을 확보하기 위해 어떤 기능을 수행해야 하는지 밑그림이 마련되어 있지 않다는 점이다. 물류보안에 민간기업의 참여를 높이기 위한 지원방안이나 물류보안 기술 개발 및 보급을 촉진하기 위한 정책도 아직은 전무한 실정이다. 물류보안 전문 인력을 양성하는 방안도 기존 법률에는 반영되어 있지 않다.

따라서 이 같은 문제점을 해결하기 위해 두 가지 법률 정비방안을 제시한다. 첫째, 국제선박 및 항만시설 보안에 관한 법률을 개정하여 범 부처간 물류보안업무를 통합·조정하는 규정을 삽입한다. 또한 이 법률에 국가물류보안 계획의 수립과 시행에 관한 규정뿐만 아니라 물류보안에 참여하는 민간기업의 지원 및 물류보안을 촉진할 수 있는 내용도 반영한다. 이 같은 방안을 선택하는 경우 기존 법률을 개정하는 형식을 취하기 때문에 새로운 법률을 제정하는 방식보다 용이하다는 장점이 있다. 그러나 이 법률은 기본적으로 ISPS 코드를 이행하기 위해 제정되었기 때문에 한계가 있다. 위에서 언급한 사항을 반영하기 위해서는 별도의 장을 신설해야 하는데, 법률의 형식과 법률 내용에 일관성이 없다는 비판에 직면할 수 있다.

둘째, 따라서 이 같은 문제점을 해결하는 대안으로 신규 법률을 제정하는 방안도 검토해볼 필요가 있다. 즉, 가칭 ‘물류보안 촉진 및 지원에 관한 법률’을 제정해 앞으로 우리나라가 추진해야 하는 물류보안정책을 제도화하는 방안이다. 신법을 제정하는 경우에는 i) 법률의 제정목적, ii) 물류보안에 관한 정부 및 민간부문의

의무와 책임, iii) 이 법률에서 사용되는 용어에 대한 정의, iv) 물류보안에 관한 각 정부 부처의 권한과 관장업무, v) 각 부처 차관 급으로 구성되는 물류보안위원회의 설치·운영, vi) 국가 물류보안 계획의 수립·시행, vii) 물류보안 인증제도의 도입, viii) 물류보안 조사 및 연구 개발, ix) 물류보안 전문 인력의 육성, x) 물류보안 참여업체에 대한 지원, xi) 물류보안 장비 및 기술 개발 투자와 지원, 예산의 확보, xii) 물류보안 정보시스템 구축, 그리고 외국과의 물류보안 협력 등에 관한 사항을 규정하면 될 것으로 보인다. 물류 전구간의 안전을 확보하기 위한 물류보안 시스템의 구축·운영 등에 관한 사항도 이 곳에서 반영하면 된다.

다만, 이 같은 방안을 추진하는 경우에는 신법 제정에 따른 절차의 복잡성, 기존 법률과의 일부 조항 상충 여부, 그리고 특정 부처에서 입법을 추진하는데 따른 타 부처의 반발 등도 있을 것으로 예상된다.

3) 물류보안 인증제도의 도입

미국이 C-T PAT를 2002년 초부터 도입한 이후 국제적으로 물류보안 인증제도가 더욱 확산되고 있다. WCO가 미국의 C-T PAT와 CSI를 결합한 형태인 SAFE Framework를 2005년 8월에 도입한 데 이어 유럽연합과 싱가포르, 일본 등 주요 국가들이 이 제도를 속속 시행하고 있기 때문이다. 또한 이들 국가들은 자체적으로 물류보안 인증제도를 도입하는 한편, 물류보안 인증을 상호 인정하도록 하는 외교적인 협력도 강화하고 있다. 한 나라에서 물류보안 인증을 받은 기업이 다른 나라에서 추가적인 인증 없이도 기존의 자격을 그대로 인정해주는 것이 절차를 간소화하고, 비용부담을 줄일 수 있기 때문이다. WCO의 SAFE Framework에 명시되어 있는 Pillar I(세관 대 세관협력)도 이 같은 내용을 뒷받침하고 있다.

우리나라에서 물류보안 인증제도를 시행하기 위해서는 몇 가지 준비작업이 필요하다.

첫째, 이 제도를 시행하기 위한 법적인 근거를 마련해야 한다는 점이다. 즉, 물류보안 인증제도에 대한 개념을 적시하고, 인증심사 업무를 담당할 기관을 지정하거나 새로 설립하는 절차가 수반되어야 한다. 또한 인증에 참여하는 기업에 대해 인센티브를 제공하는 방안도 아울러 강구해야 한다. 이 같은 사항은 앞에서 언급한 법률 제정 및 개정 방안에 포함하면 된다.

둘째, 인증에 참여하는 기업이나 단체를 어디까지 한정해야 할지 정해야 한다는

점이다. 현재 물류보안 인증제도를 도입한 미국이나 WCO의 경우 참여 기업에 대한 범위가 각각 다른 것이 특징이다. 미국의 경우 수입업자, 운송인, 컨테이너 터미널 운영업체 등 6개 부문으로 한정하고 있는 반면, WCO는 화물의 국제교역에 종사하는 모든 기업이나 업체를 대상으로 망라하고 있다. 민간 기업의 보다 폭넓은 참여를 유도하기 위해서는 인증 대상을 확대하는 것이 바람직한 것으로 보인다. 다만, 이렇게 할 경우에는 적정 수준의 인증심사원을 확보하지 않으면, 인증심사가 지연되는 폐해가 발생할 우려가 있다.

셋째, 물류보안 인증제도를 시행하기 위해서는 참여 대상 기업이 준수해야 하는 물류보안 인증기준이 필요하다. 즉, 제조업체나 창고업체 또는 운송인 등이 각각 지켜야 하는 최소한의 물류보안 요건이 마련되어야 한다는 점이다. 미국의 경우 각 부문별로 최소한의 물류보안 인증기준(minimum requirement)을 설정해 놓고, 이 기준을 적절하게 이행하고 있는지 심사한 뒤 자격을 부여하고 있다. 그러나 유럽 연합이나 싱가포르 등은 각 부문별로 물류보안 인증기준을 정하지 않고, 포괄적인 기준을 마련하여 시행하고 있다. 완벽한 물류보안 인증제도를 도입한다는 관점에서는 미국의 제도가 바람직한 것으로 보인다. 이 보고서에서는 후자의 예에 따라 물류보안 인증기준을 마련, 부록으로 첨부하였다.

넷째, 물류보안 인증 심사를 정부에서 담당할지 아니면 특수 민간기관에 위탁하게 할지 결정해야 한다는 점이다. 전자에 따를 경우 정부 부처 내에 별도의 조직을 신설해야 하는 문제가 있다. 민간기관에 위탁하여 시행하게 하는 경우에는 법률에 따라 단일 또는 복수의 인증심사 기관을 지정해야 한다. 미국의 경우는 정부조직인 세관·국경 보호청(CBP)에서 담당하고 있다. 이에 비해 유럽연합의 경우는 자격 요건을 충족하는 민간기관이 물류보안 인증심사에 참여하는 길을 터놓고 있다. 작은 정부를 지향하는 측면에서 보면, 일정한 자격을 갖춘 민간부문에 인증심사를 위탁하는 것이 바람직하다.

다섯째, 물류보안 인증업무를 한 개 정부부처에서 담당할지 아니면 소관업무별로 담당부처를 다양화할지 신중하게 검토해야 한다는 점이다. 우리나라 정부 조직법상 물류보안제도 시행과 관련되어 있는 정부부처는 산업자원부, 건설교통부, 해양수산부, 국가정보원, 재정경제부(관세청) 등 다양하다. 이들 정부 부처는 현재 소관업무별로 물류보안제도를 시행하고 있거나 시행하는 방안을 각각 마련하고 있다. 따라서 어느 한 부처에서 물류보안 인증제도를 도입하는 경우 다른 부처의 소관업무까지 침해하는 결과를 초래할 우려가 있다. 가장 바람직한 방법은 특정

법률에 물류보안 인증제도를 도입하기 위한 근거를 마련하고, 소관부처별로 각각 해당민간기업의 물류보안 인증업무를 수행하도록 하는 것이다. 일본이 현재 이 같은 방식을 택하고 있다.

4) 완벽한 물류보안 시스템 구축

물류보안은 제도 도입만으로 완성되지 않는다. 제도를 뒷받침할 수 있는 하드웨어, 즉 물류보안 시스템을 구축하지 않으면, 사상누각과 다를 바 없다. 현재 나와 있는 각종 기준을 조합해 볼 때 완벽한 물류보안 시스템을 구축하기 위해서는 크게 인적 및 물적 보안시스템을 마련하는 것이 시급하다.

우선, 인적 보안시스템 구축과 관련해서는 근로자에 대한 주기적인 신원조사와 인가 받지 않은 사람이 제한구역에 접근하는 방법을 차단하는 방안을 마련하는 것이 시급하다. 전자에 대해서는 현재 일부 기업이 근로자를 고용할 때 관계 기관의 협조를 받아 시행하고 있으므로 물류보안 인증심사 기업에 확대해도 무방할 것으로 보인다. 그러나 신원조사를 제한적인 범위에서 시행하지 않는 경우에는 사생활을 침해할 소지도 있다는 점에 유의할 필요가 있다. 인가되지 않는 사람에 대한 접근 통제는 출입증을 발급할 때 방문지역을 제한하고, 이를 어기는 경우 경고할 수 있는 추적 모니터링 시스템을 설치해야 한다.

한편, 물적 보안 시스템을 구축하기 위해서는 현재 나와 있는 물류보안제도가 무엇을, 어디까지 요구하고 있는지 파악하는 것이 선행되어야 한다. 지금의 물류보안제도는 물건을 제조하는 단계에서 최종 소비지까지 이르는 전 구간의 완벽한 안전 시스템을 갖추도록 하고 있다. 즉, 화물이 제조업체와 물품을 보관하는 창고, 철도와 도로 등 내륙운송수단으로 이어지고, 항만을 통해 다른 나라로 운송되어 도착할 때까지 테러 차단과 안전을 담보하도록 요구하고 있는 것이 현실이다.

즉, 각종 제조업체나 물류창고 등의 시설에 대해서는 담장이나 출입통제장치 및 조명, 감시카메라 등을 설치하는 것이 일반적이다. 그리고 화물이 운송되는 도중에 부정개폐를 방지하는 봉인장치와 부정개폐되는 경우 이를 화주나 터미널 운영업체, 또는 관련 기관에 전자적으로 통보할 수 있는 화물 추적시스템을 갖추고 있어야 한다. 컨테이너 화물이 항만에 도착할 때에는 화물 명세 등을 신고할 수 있는 물류보안 정보 시스템과 컨테이너 화물 검색기와 검색 결과를 전송하는 물류정보망도 갖추도록 한다. 앞으로 해양수산부와 산업자원부, 정보통신부 등 유관 정부

부처간에 협의를 거쳐 오늘날 물류보안제도가 요구하는 사양에 맞춰 ‘물류보안 패키지 시스템’을 결정하는 것도 필요하다.

5) 물류보안산업의 육성 및 지원

완벽한 물류보안 시스템을 구축하기 위해서는 이에 걸 맞는 기술과 장비 및 소프트웨어 등 일정한 물류보안 솔루션을 개발하고 보급하는 것이 중요하다. 즉, 물류보안 시스템을 구축하기 위해서는 시설물의 출입통제장치(사람 및 차량)와 컨테이너 화물 추적시스템, 컨테이너 전자 봉인장치(CSD 포함), 화물검색기, 방사능 탐지기 등이 기본적으로 설치되어 있어야 한다. 특히 미국이 2007년 9·11 테러 대책이행법률을 제정함에 따라 앞으로 2012년 7월까지 미국으로 화물을 수출하는 모든 나라는 컨테이너 화물을 100% 검색할 수 있는 검색기를 항만에 설치해야 한다. 따라서 항만에서 체증현상 없이 화물을 안전하고, 신속하게 처리해 수출하는 게 중요한 과제로 등장하였다.

문제는 현재 우리나라가 갖고 있는 수준이나 시장 동향을 볼 때 이 같은 물류보안 솔루션을 완벽하게 구축할 수 있는 여건을 확보하지 못하고 있다는 점이다. 컨테이너 화물 추적과 전자 봉인장치, 물류정보 시스템 등은 사비 네트워크와 제너럴 일렉트릭(GE)을 중심으로 하는 글로벌 대기업이 장악하고 있다. 컨테이너 화물 검색기도 미국의 SAIC와 스미스 디텍션 사, 그리고 중국의 누크테크 등이 시장을 3분하고 있는 형국이다. 즉, 이 같은 현실을 고려할 때 우리나라 물류보안 시장은 선진국에 기술적으로 경제적으로 종속될 우려가 매우 커졌다고 할 수 있다. 중국의 경우 자체적으로 컨테이너 화물 검색기를 개발, 해외에 수출하고 있고, 독자적인 컨테이너 봉인장치를 상용화하고 있는 점과 비교된다.

앞으로 우리나라는 시장 규모가 크게 확대될 것으로 판단되는 i) 컨테이너 화물 추적 및 전자 봉인장치를 포함한 스마트 컨테이너 개발, ii) 100% 검색제도가 도입됨에 따라 고속·고선명이 경쟁력으로 등장하게 될 컨테이너 화물 검색기, 그리고 컨테이너 화물 정보를 포함한 물류 정보를 수집·가공·분석하고, 제공하는 물류보안 정보 시스템을 개발하고, 보급하는 데 역점을 뒀야 한다. 특히 마지막 사항의 경우는 전자와 서로 연계되는 것으로 향후 기업에 상당한 부가가치를 창출할 수 있는 분야로 평가되고 있으므로 정책 당국의 적극적인 기술 개발 지원이 필요하다.

또한 미국의 경우 자국으로 수출하는 모든 컨테이너 화물에 대한 검색을 의무

화하면서 이에 사용하게 될 화물 검색기에 대한 표준을 제정할 방침으로 있다. 미국의 이 같은 방침이 현실화될 경우 기존에 우리나라에 설치되어 있는 10대 이상의 화물 검색기는 무용지물이 되거나 기능이 상당부분 제한될 우려도 있다. 이에 그치지 않고, 미국의 표준이 미국 컨테이너 화물 검색기 제조업체에 유리하게 작성되는 경우 기술 종속과 기술 사용료 지출도 늘어날 것으로 보인다. 국제 표준화 기구 등과 함께 컨테이너 화물 검색기에 대한 국제 표준을 우리나라 주도로 수립해야 한다.

6) 국가경쟁력에 물류보안을 활용

2001년 9·11 테러 이후 물류보안을 확보하기 위한 여러 가지 제도가 쏟아져 나왔다. IMO를 중심으로 선박과 항만의 보안제도가 마련되었고, 미국과 WCO가 힘을 합쳐 컨테이너 화물 사전검색제도와 물류보안 인증제도를 창출하였다. 글로벌 대기업은 ISO와 손을 잡고, 컨테이너 화물 봉인장치를 국제표준으로 만드는 데 성공하였다.

이에 따라 앞으로 국제교역은 이 같은 제도를 어느 정도 신속하게 이행하느냐에 따라 국가별로 경쟁력이 판가름나게 되었다. 기술과 자본을 갖고 있는 나라는 완벽한 물류보안 시스템을 갖추으로써 다른 나라에 앞서 경쟁력을 확보할 것이 분명하다. 글로벌 물류허브 성장전략을 추진하고 있는 싱가포르와 홍콩의 경우 물류보안을 자국의 물류경쟁력을 활용하는 방안으로 적극 추진하고 있다. 인근의 다른 항만과 경쟁하고 있는 컨테이너 터미널 또한 이와 별반 다르지 않다.

대표적인 세계 컨테이너 터미널 운영업체 가운데 하나인 디피 월드(DP World)의 경우 세계에서 처음으로 ISO/PAS 28000을 근거로 제벨 알리 항만에 대한 보안 인증을 받은 데 이어 운영하고 있는 다른 항만까지 인증을 확대한다는 계획이다. 이 같은 방침에 따라 디피 월드가 대주주로 있는 우리나라 부산 신항만 주식회사(PNC)도 한국선급의 사업장 보안인증을 받고 있다. 자사 터미널이 완벽한 보안시스템을 갖추고 있는 경우 기항 선사가 늘 것으로 예상될 뿐만 아니라 선사 마케팅에도 활용할 수 있는 이점이 있기 때문이다.

홍콩의 모던 터미널 주식회사는 자사가 운영하는 모던 터미널을 뒤늦게 미국 항만보안법에 따른 컨테이너 화물 100% 검색 시범사업에 참여시키고 있다. 미국은 2006년 말에 이른바 SFI(Secure Freight Initiative)를 도입하면서 대상항만을 우리

나라 부산항의 허치슨 감만 터미널 등 6개 항만으로 한정하였다. 그러나 홍콩 모던 터미널은 컨테이너 화물 검색기의 오작동을 불러일으키는 부두 콘크리트를 전면 교체하고, 시범사업에 참여하고 있다. 완벽한 화물 검색이 이뤄지면, 양륙항만에서 통관 절차 등이 간소화되어 화물 유치에 크게 기여한다는 판단에 따른 것이다.

우리나라의 경우 일본이나 중국 항만 등 인접 국가와 컨테이너 화물 유치에 사활을 걸고 있다. 미국의 컨테이너 화물 100% 사전 검색 의무화는 우리나라에서 발생하는 화물은 물론 환적 화물의 검색도 동시에 요구하고 있다. 우리나라 항만에 완벽한 물류보안 시스템을 갖추는 경우 우리나라 항만의 경쟁력이 높아질 뿐만 아니라 중국 환적 물동량을 유치하는 데도 기여할 것으로 보인다. 우리나라 항만에 물류보안 시스템을 신속하게 구축하여 항만 마케팅 등에 적극적으로 활용할 필요가 있다.

7) 물류보안 연구센터 설립·운영

전세계적으로 물류보안제도가 강화되고 확산되는 상황에 적극적으로 대처하고 물류보안산업을 정책적으로 지원하기 위해서는 물류보안 연구센터가 필요하다. 현재 논의되고 있는 물류보안 전담조직은 물류보안 업무를 관리하고 집행하는 역할을 하고, 이와는 별도로 국제적으로 논의되고 있는 물류보안제도를 분석하고 국내대책을 수립할 수 있는 기구가 있어야 한다.

즉 행정집행조직과 별도로 분리된 물류보안 연구센터를 설립하여 물류보안제도의 동향파악과 대책수립, 국내 물류보안산업 발전방안 수립, 물류보안에 관한 국제기준 제정 참가, 물류보안인력 교육훈련 지원, 물류보안관련 법률 정비, 물류보안 민간 컨설팅 업무 등을 전담하여야 한다. 특히 물류보안은 국제표준으로 제정되고 있어 이에 대한 각국의 이해를 적절한 시기에 반영하지 못할 경우 민간기업의 물류비용 증가와 수출입 경쟁력이 저하될 가능성이 매우 높다.

물류보안 연구센터는 업무의 영속성과 전문성을 고려하여 물류보안 전문 연구기관 산하에 두고, 물류보안을 주관하는 부서의 예산으로 운영해야 한다. 물류보안연구는 연구 특성상 민간의 수요가 많지 않고 수익이 발생할 소지가 거의 없다. 따라서 정부에서 이에 필요한 경상비를 지원하는 방식으로 운영해야 한다.

8) 민간 부문의 부담완화도 필요

물류보안은 9·11 테러라는 다른 나라에서 발생한 외생 변수로 인해 국제적으로 도입된 제도이다. 따라서 이 제도가 테러 예방과 차단을 통한 인명과 재산을 보호하고, 글로벌 교역 질서를 지킨다는 대의명분에도 불구하고, 실제 시행하는 정부와 민간 기업에 대해서는 적지 않은 부담을 주고 있는 것이 사실이다. 우리 원이 2006년에 개최한 물류보안 세미나에서 한국선주협회와 한국무역협회 등 관련 업계에서는 이 같은 부담을 줄일 수 있는 방안을 강력하게 요구하였다. 정부가 2007년에 국제 항해선박 및 항만시설에 관한 법률을 제정하면서 항만시설 보안료 부과 및 징수에 관한 규정을 3년 동안 유예한 것도 이 같은 업계의 요구를 반영한 결과이다. 앞으로 물류보안 인증제도를 도입하고, 항만 물류보안 시스템을 구축하는 과정에서 관련 업계가 입을 수 있는 피해를 최소화하고, 인센티브 제공 등 부담을 줄이는 노력이 필요하다.⁹⁹⁾

3. 정책 추진 일정표(로드맵)

한편, 본 보고서에서 제시한 정책 제언 사항을 구체화하기 위해서는 일정한 정책 추진 일정표(로드맵)가 필요하다. 물류보안에 관한 국제적인 흐름과 예산 및 관련 업계의 준비 상태 등 여러 가지를 고려하여 업무 추진 우선순위를 가리는 것이 바람직하기 때문이다. 따라서 이 곳에서는 기존 제도를 보완하고, 업계의 요구 사항 등을 토대로 다음과 같은 로드맵을 작성하였다.

첫째, 국가물류보안계획은 2008년 중에 수립·시행하는 것이 바람직하다. 각 부처에 분산되어 있는 물류보안업무를 통합적인 관점에서 집행하기 위해서는 해양수산부 등이 중심이 되는 법정 계획이 필요한 까닭이다. 이 계획은 해양수산부와 건설교통부, 그리고 관세청 등 물류보안 관련 부처가 공동으로 참여한 가운데 수립하는 것이 향후 업무 시행과정에서 집행력을 제고할 수 있다.

둘째, 물류보안 법률의 제정과 개정은 2010년까지 추진해도 무방할 것으로 판단된다. 이에 앞서 국가물류보안계획이 수립되어 시행되므로 업무 추진 우선순위를

99) 물류보안제도를 도입하는데 따른 민간기업의 의견에 대해서는 2006년 보고서(225면) 이하 참조할 것.

뒤로 미루어 두어도 큰 지장을 초래할 것으로 보이지 않기 때문이다. 다만, 법률의 제·개정과 관련하여 향후 고려해야 할 점은 신법을 제정하는 경우 기존에 해양수산부에서 제정한 법률과의 관련 등에 대해서 면밀한 검토가 필요하다는 점이다.

셋째, 물류보안 인증제도 도입은 가장 시급하게 서둘러야 할 부분이다. WCO 등에서 이에 관한 국제기준을 채택한 이후 이 제도를 시행하는 국가가 늘어나고 있고, 화물을 수출하는 기업의 입장에서는 신속 통관 등 이해관계가 가장 크기 때문이다. 해양수산부, 건설교통부, 관세청 등이 적극 나서서 추진해야 하는 제도로 판단된다.

넷째, 완벽한 물류보안 시스템은 국제적으로 강제되는 사항을 고려하여 2010년까지 추진하는 것으로 한다. 특히 이와 관련하여 문제가 될 수 있는 부분은 미국이 2010년 7월부터 자국으로 수입되는 모든 컨테이너 화물에 대한 100% 사전검색을 의무화한 점이다. 따라서 이 같은 일정에 맞추기 위해서는 그 전에 컨테이너 화물 검색시를 포함한 물류보안 시스템을 설치·운영하여야 한다.

<표 6-1>

정책 제언 사항 추진 로드맵

정책 제언 사항	추진 시기			추진방법
	2008년 까지	2010년 까지	2012년 까지	
1. 국가물류보안계획 수립·시행	○			관련부처 법정계획으로 추진
2. 물류보안 관련 법률 제·개정		○		해양수산부, 건설교통부 등이 신법 제정
3. 물류보안인증제도 도입·시행	○			관세청·해양수산부, 건교부 등이 기준 제정 후 사업 시행
4. 완벽한 물류보안시스템 구축		○		항만부터 시스템 구축 후 전 물류구간으로 확대
5. 물류보안산업의 육성·지원	○	○	○	가능한 사업부터 단계적으로 추진
6. 국가경쟁력에 물류보안 활용		○		제시한 국가 물류보안계획에 반영하여 추진
7. 물류보안연구센터 설립·운영	○			물류보안전문연구기관 조직으로 설립

자료 : 한국해양수산개발원

다섯째, 물류보안산업을 육성하고 지원하는 일은 2008년부터 지속적으로 추진하는 것으로 한다. 컨테이너 화물 검색기와 컨테이너 전자 봉인장치, 화물 추적 시스템 등 물류보안을 물리적으로 확보하는데 필요한 기술과 장비 개발이 용이하지 않기 때문이다. 물류보안산업의 육성 및 지원은 산업자원부와 해양수산부, 정보통신부 등이 ‘중장기 국가 성장전략’으로 채택하는 방안도 검토할 필요가 있다. 미국의 SAIC 등 글로벌 기업들은 국토안보부의 강력한 예산 지원을 바탕으로 첨단 물류보안 솔루션을 개발, 세계 시장을 장악하고 있다.

여섯째, 물류보안의 지속적 발전과 완벽한 대책 수립을 위해서는 이에 대한 대책이 계속 수립되어야 한다. 이를 위해서는 현재 연구 프로젝트 중심으로 수립하는 대책을 상설적인 연구조직에 의해 계속적으로 진행할 수 있도록 시스템을 마련해야 한다. 이를 위해 물류보안 전문연구기관 내에 우선 ‘물류보안연구센터’를 운영할 수 있도록 관련기관의 지원이 필요하다. 그리고 중장기적으로 ‘물류보안연구센터’가 독자적인 준립기반을 마련할 수 있도록 하면서 민간 프로젝트 개발, 물류보안교육 및 컨설팅 기능을 강화해야 한다.

참 고 문 헌

- 목진용, “항만시설 경비보안제도의 개선방안”, 「해양수산」, 제251호, 한국해양수산개발원, 2005. 8.
- 민성규, “미국의 컨테이너 보안 프로그램 C-T PAT, CSI, 선적 24시간 전 화물 정보 신고규칙”, 「해양한국」, 해사문제연구소, 2003. 9.
- 박준석, 「뉴테러리즘개론」, 백산출판사, 2006. 2.
- 부산항부두관리공사·한국로지스틱스학회, 「항만경비보안세미나」, 2006. 12. 15.
- 석창부, 물류보안시스템 구축방안, 한국해양수산개발원, 내부세미나 자료, 2007. 9.
- 여영무, 「국제 테러리즘 연구 : 고대 로마부터 오사마 빈 라덴까지」, 한국해양전략연구소, 2006.
- 이갑수, 「글로벌시대의 선업정책론」, 도서출판 대명, 2007.
- 이석기, “전략물자 수출통제와 관련된 기업인증제 실시 전망과 대책”, KTET. 2006년 1월.
- 일본기계수출조합, 「서프라인체인 보안프로그램의 국제비교」, 2006. 6.
- 정대율, “2005년 항해안전에 대한 불법 억제협약의 국내대응방안 연구”, 「해사법연구」, 제18권 제1호, 한국해사법학회, 2006. 3.
- 지이보안(GE Security) 부문 사장의 인터뷰 내용, <http://tong.nate.com/raccoon1128/29104954>.
- 최운덕, 컨테이너용 전자봉인장치(E-seal) 기술개발 및 시장동향, 한국해양수산개발원 내부세미나 자료, 2007. 8.
- 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.
- _____, “유엔 결의(1718호)에 따른 북한 선박 및 화물 검색은 가능한가?”, 「KMI 해양수산 현안분석」, 한국해양수산개발원, 2006. 11.
- _____, “중국의 항만 보안료 부과와 시사점”, 「해양수산동향」, Vol, 1222, 한국해양수산개발원, 2006. 8. 2.
- _____, “최근의 해사보안 강화 동향과 정책 시사점”, 「KMI 해양수산 현안분석」, 한국해양수산개발원, 2002. 10.

- _____, “해상안전과 보안 동향 전망”, 「해양한국」, 한국해사문제연구소, 2005. 1.
- _____, “IMO 해사보안협력 시행방안”, 「KMI 해양수산 현안분석」, 한국해양수산개발원, 2003. 3.
- _____, “ISPS Code(선박 및 항만시설 보안규정)가 왜 문제인가”, 「해양수산동향」, Vol. 1143, 한국해양수산개발원, 2004. 5. 3.
- _____, “컨테이너 화물 100% 사전 검색의무화와 정책 시사점”, 해양수산현안분석, 한국해양수산개발원, 2007. 8. 6.
- _____, “최근의 물류보안 강화 동향”, 「물류보안 대책 마련을 위한 대토론회」 자료집, 한국무역협회 · 한국해양수산개발원, 2006. 10. 17.
- 최진태, 「항공테러리즘의 이론과 실제」, 대영문화사, 2006. 6.
- 한국무역협회 · 한국하주협의회 · 한국해양수산개발원, 「물류보안 대책 마련을 위한 대토론회」, 2006. 10. 17.
- 한국해양수산개발원, 「국가물류보안체제 확립방안 연구(I)」, 2006.12.
- 한국해양수산개발원 외, 국제 물류보안 동향 및 대응 전략 세미나 자료, 2007. 10. 23.
- 한국해양수산연수원, 「ISPS Code의 국내수용방안 연구」, 해양수산부, 2006. 7.
- 한국표준, KS A ISO 9001 : 2007, 품질경영시스템.
- _____, KS A ISO 14001 : 2004, 환경경영시스템.
- _____, KS A ISO 20858 : 2007, 해운 항만시설의 보안평가 및 보안계획서 개발.
- _____, KS V ISO 28000 : 2007 공급관리 보안경영시스템 .
- _____, KS V ISO 28001 : 2007.
- _____, KS V ISO 28004 : 2007.
- 항공보안교육원, 「제3회 항공보안세미나」, 2006. 11. 30.
- 해양수산부, 「항만시설보안지침서 개발연구」, 2004. 9.
- 황진희, “주요국의 물류보안 강화동향과 대응방안”, 「항만보안경비세미나」, 한국로지스틱스학회 · 부산항부두관리공사, 2006. 12. 15.

- KS A ISO 9001:2007, 품질경영시스템 -요구사항.
- KS A ISO 14001:2004, 환경경영시스템 -요구사항 및 사용지침.
- KS A ISO 19011:2007, 품질경영시스템 · 환경경영시스템 심사 지침.
- KS A ISO 20858:2007, 해운 항만시설의 보안평가 및 보안계획서 개발.
- KS V ISO 28001:2007, 공급사슬 보안경영시스템? 공급사슬의 보안, 평가 및 계획의 실행을 위한 모범관행? 요구사항 및 지침[6] KS V ISO 28004 : 2007,

- 공급사슬 보안경영시스템 - KS V ISO 28000 실행지침.
- 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.
- APEC, APEC Private Sector Supply Chain Security Guidelines, 2007. 5.
- APEC, Papers for APEC Symposium on Total Supply Chain Security, 2006. 7.
- Ashley Roach JAGC, "Container and Port Security : A Bilateral Perspective", *The International Journal of Marine and Coastal Law*, vol. 18. No. 3, 2003.
- Brian Robinson, *Testing time for box checks*, Cargo Systems, 2006. 6.
- _____, *Towards a disposable seal*, Cargo Systems, 2006. 6.
- C ARIEL PINTO AND WAYNE K. TALLEY, "The Security Incident Cycle of Port", *Maritime Economics & Logistics*, 2006. 8.
- Container Internationalization, 2007. 6. 18.
- DOH, *The National Strategy of Maritime Security*, 2006. 9.
- Global Leaders Institute, *PorTech Asia 2006*, 2006. 9.
- Drewry Shipping Consultants Ltd, *Annual Container Market Review and Forecast 2006/7*, 2007.
- Fairplay, 2006. 6. 8.
- Frost & Sullivan, *Container Security - A Market Analysis*, 2007. 3.
- Hartmut G. Hesse, Maritime Security in Multilateral Context : IMO Activities to Enhance Maritime Security, *The International Journal of Marine and Coastal Law*, vol. 18. No. 3, 2003.
- Herry. H. Willis, David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, RAND Corporation, 2005. 5. 25.
- Journal of Commerce, 2007. 6. 4., 2007. 4. 10., 2006. 4. 25.
- Kilman, Daniel M, *Japan's security strategy in the post-9/11 world*, McGraw Hill, 2006.
- Maritime Policy and Management, January-March, 2005.
- OECD, *Container Transport Security Across Modes*, 2004.
- RUTH BANOMYONG, "The impact of port and trade security initiative on maritime supply-chain management", *Maritime Policy and Management*, Vol. 32, No. 1, Jan-Mar, 2005.
- Savi, *Eseal Specification and Solution*, Interior Materials, 2007. 4.

VIAN V THAI and DEVINDER GREWAL, "The Maritime Security Management System : Perceptions of the International Shipping Community", *Maritime Economics & Logistics*, 2007. 9.

부록 : 싱가포르 및 ISO의 물류보안 인증제도

부록 1**싱가포르 STP 가이드라인****1. 머리말**

- 1.1 STP 가이드라인은 공급관련 업체들이 자신들의 업무처리와 공급 체인의 보안성을 증진시키기 위해 갖추어야할 조건들을 제시하고 있다. 제시된 조건들을 충족시킨 업체들은 싱가포르 세관에 의해 STP 업체로 인증 받을 것이다.
- 1.2 STP가이드라인에 따르면 업체들은 다음과 같은 조건을 충족해야 한다.
- (a) 보안 관리 시스템을 갖추어야 한다.
 - (b) 자신들의 작업수행에 대한 위험 평가를 실시해야 한다.
 - (c) STP가이드라인에 따라 보안조치를 취하여 유통라인의 보안을 확보해야 한다.
- 1.3 STP 가이드 라인은 업체들에게 그들의 유통라인의 조치와 실행들을 개발하고 실행하며 감시하고 검토할 수 있도록 개괄적인 틀을 제공한다.
- 1.4 STP인증서를 받기로 결정한 업체들은 STP가이드라인에 비추어 자신들의 정책 처리 과정, 그리고 절차가 적절한지 자체 평가를 해야 할 것이다.

2. 보안 관리 시스템

- 2.1 유통업체보안은 그 업체 내 속한 한 개인이나 부서만이 부담하는 독립된 책임일 수 없다. 확고한 유통 업체 보안 조치를 달성하기 위해서는 보안이 업체 내 모든 구성원들이 노력해야만 한다.
- 2.2 공급업체는 자신의 유통라인의 보안 조치와 실행 등을 개발하고 기록하고 유지하며 검토할 수 있도록 보안 시스템을 구축해야 한다. 보안 관리 시스템은 다음을 포함하지만 여기에 한정되지는 않는다.

- (a) 업체의 보안 정책, 목적, 보안 조치를 구축하고 검토할 수 있는 개괄적인 체계
- (b) 업체내 효과적인 의사소통을 위한 체계
- (c) 지속적으로 보안 적합성 검토하고 개선을 담보할 수 있는 검토 체계

3. 위험평가

3.1 STP는 업체들이 업체 유형에 따른 위험 평가에 기초해 보안 정책을 수립하고 보안 조치를 실행할 수 있도록 해준다.

3.2 업체는 작업과정과 공급 체인의 위험평가를 해야 한다. 그래서 공급 체인내의 작업 시 위험요소와 취약요소를 줄이도록 해야 한다.

제조업자/공급업자

3.3 제조업자와 공급업자는 대개 완제품의 유통라인에 있어 출발점에 있다. 그들의 공장에 들어오는 원자재와 상품이 처음부터 제대로 기록되어야 악용될 수 있는 데이터 오류나 나중의 유통단계에서 내용물 검증 필요성을 최소화할 수 있다. 정확한 적하목록, 변형방지 포장, 잘 기록된 양도 과정을 통해 제조업자와 공급업자들은 창고 관리자와 운송업체 같은 화물 처리 업체에 물품을 정상상태로 넘겨주어야 물품들이 안전하게 공급 체인에 넘겨질 수 있다.

창고 관리자와 소유주

3.4 창고 관리자와 소유주들은 제조업자나 운송업체 또는 다른 중개업자로부터 물품을 받아 다른 중개업자에게 전달하거나 종종 다른 형태로 전달한다. 화물처리 업체들은 적절한 정보 시스템을 보유하여 자신들이 다루는 모든 물품들을 기록할 수 있어야 하고 물품에 관련한 정보를 다음 단계의 공급업자에게 제공할 수 있어야 한다. 게다가 자신들에게 맡겨진 물품들이 훼손 변경으로부터 안전하도록 관련시설이 적절히 유지되어야 한다.

운송업자

3.5 운송 책임자들은 물품을 한 지점에서 다른 지점으로 운반하는데 주요한 책임을 지고 있다. 운송업자들은 자신들의 운반 수단이 납치되거나 바뀌치기 당하지 않도록 수단을 강구해야 한다. 운송업자들은 적절한 정보 시스템을 통해 자신들에게 맡겨진 물품들을 감시하고 추적해야 한다. 게다가 운송업자들은 자신들의 운송수단과 자신들이 운반한 물품들이 쉽게 변형되지 않도록 해야 한다.

3.6 터미널 운영자들은 물품을 비행기나 선박에 싣기 전과 내린 후에 물품과 컨테이너를 취급하는데 주요한 책임이 있다. 본래 터미널은 물품과 컨테이너가 떠나기 전에 마지막 지점이고 도착 시에는 첫 번째 지점이다. 그래서 터미널 시설은 안전하게 관리되어 터미널에 맡겨진 물품들이 훼손 변경되지 않도록 해야 한다.

수상과 항공 운송업자

3.7 수상과 항공 운송업체들은 물품을 선박과 항공기를 통해 각각 한 지점에서 다른 지점으로 운반하는데 핵심적인 역할을 한다. 수상 항공 운송업체들은 운반도중에 납치되거나 바뀌치기 당하지 않도록 해야 한다. 수송업체들은 적절한 정보 시스템을 통해 자신들에게 맡겨진 물품들을 감시하고 추적할 수 있도록 해야 한다. 게다가 수송업자들은 그들의 선박, 항공기 그리고 선박 항공기에 실린 물품들이 쉽게 변형되지 않도록 관리해야 한다.

4. 보안 조치

4.1 STP가이드라인에 따른 보안 조치들은 업체가 준수해야 하는 8가지 요소로 구성된다.

- (a) 시설 보안과 접근 통제
- (b) 인력 보안
- (c) 사업 파트너 보안

- (d) 화물 보안
- (e) 운송기관 보안
- (f) 정보와 정보 기술 보안
- (g) 사고 관리와 조사
- (h) 위기 관리과 사고 수습

4.2 채택되거나 실행된 보안 조치들이 해당 기업의 위험 평가 과정에서 확인된 위험성과 취약성을 완화하도록 해야 한다.

4.3. STP 가이드라인상의 보안조치들에 대해서는 부속서 A를 참조할 것

STP 가이드라인 - 보안 조치들

1. 시설 보안과 접근 통제

접근 통제와 물리적인 억제물을 적소에 배치하여 회사 시설물 내외부에 무단침입을 방지해야한다. 통제 시스템을 통해 모든 입구에 모든 직원들과 방문객들의 신분을 철저히 확인해야 한다.

1.1. 경계벽

경계벽과 적절한 주변 장애물들을 적소에 배치하여 회사 시설물의 보안을 유지해야 한다. 경계벽은 구역이나 터미널 특히 컨테이너, 화물 위탁, 트레일러와 화물 차량 등이 주차되고 보관되어 있는 지역들을 포괄해야 한다. 모든 경계벽을 규칙적으로 이상이 없는지 점검해야 한다.

1.2 출입구와 출입 관리 사무소

모든 차량과 사람들이 출입하는 출입구를 인원을 배치하고 감시하고 그렇지 않으면 통제해야 한다.

1.3 주차

시설내 주차허용도 통제되고 감시되어야 한다. 일반 승객 차량이 화물처리와 화물 저장 지역과 근접한 곳에 주차되지 못하도록 해야 한다.

1.4 건물 구조

건물은 불법 출입을 막을 수 있는 재료들을 가지고 건축되어야 한다. 정기적인 점검과 수리를 통해 건물의 안전을 유지해야 한다.

1.5 잠금 장치와 열쇠 통제

모든 내외부 창문, 출입문, 경계벽과 출입구는 잠금장치와 다른 감시나 통제 수단을 통해 보안이 이루어져야 한다. 관리 또는 보안 요원은 모든 잠금장치와 열쇠 발행을 통제해야 한다.

1.6 조명

적절한 조명이 회사 건물의 시설 내외부에 설치되어야 한다. 출입구, 화물, 화물 처리 및 저장지역, 경계벽과 주차 공간 등에도 설치되어야 한다.

1.7 경보 시스템과 비디오 감시 카메라

경보 시스템과 비디오 감시 카메라를 활용하여 침입자가 출입하는 것을 저지하고 무단 침입을 적발하고 보안감독 지역을 확대하고 사고사후 조사에 도움이 되도록 해야 한다.

1.8 출입 제한 지역

출입제한지역의 경우에는 무단 침입을 방지할 수 있도록 확실히 신분 확인과 함께 감시되어야 한다.

1.9 보안 요원과 기구

직원이나 부서가 그 기업의 보안을 담당해야 한다. 기업들은 시설보안을 더 강화하기 위해 보안 업체 서비스를 이용할 수도 있다.

1.10 직원들에 대한 접근 통제

철저한 신분 확인과 접근 통제 차원에서 직원 신분 확인 시스템을 갖추어야 한다. 예를 들어 직원들에게 칼라사진이 부착된 신분확인 카드를 발급해야 한다. 직원들은 자신의 업무 수행과 관련해 필요한 지역에만 출입할 수 있도록 한다.

1.11 방문객에 대한 접근 통제

방문객 신분확인 및 감시 시스템도 갖추어야 한다. 예를 들어 회사 건물에 들어 오기 전에 출입관리처에 신분증을 제시하고 등록해야 한다. 그리고 임시 신분증을 보일 수 있도록 착용해야 한다. 모든 방문객들은 그들이 적법한 사무를 가진 지역에만 안내되고 출입할 수 있다.

1.12 권한 없는 인물 조사(challenging)와 제거

모든 직원들이 허가받지 않거나 신분이 확인되지 않은 사람들을 보고하고, 조사할 수 있는 절차를 마련되고, 이에 대비한 훈련이 이루어져야 한다.

2. 인원(personnel)¹⁾ 보안

잠재적 고용인을 심사하고, 주기적으로 현재 고용인을 검사하기 위해 절차가 마련되어야 한다. 안전정책에 대한 고용인의 교육, 정책 이탈에 대한 인식 및 안전 착오 발생시 행동대책을 위한 절차도 마련되어야 한다.

2.1. 채용 전 검증, 신원 조회 및 조사

과거 채용 정보, 신원조회 및 학업 성적과 같은 지원 정보는 채용 전에 심사되어야 한다.

신원 조회와 조사는 국내법상 적절한 수준을 넘지 않는 수준에서 잠재적 고용인들에 대해 이루어져야 한다. 근무 범위 그리고/또는 기업들의 운영을 위태롭게 하는 근무배치의 민감성에 따라 잠재적 고용인들에 대해 보다 깊이 있는 신원조회 및 조사가 필요하다.

1) 한글로 옮기는 데 있어 약간 애매한 단어들은 괄호 안에 영어 단어를 표기하였음. 이하 동일.

2.2. 현 고용인들에 대한 주기적 신원조회 및 재조사

목적(cause) 그리고/또는 고용인들 직급의 민감성에 따라 현 고용인들에 대해서도 주기적인 신원조회/조사가 실시되어야 한다. 고용인들의 사회적/경제적 상황의 일상적이지 않은 변화를 참고하여 업체들은 개인 사원 파일에 있는 정보를 최신화해야 한다.

2.3. 교육, 훈련 및 인식 제고(awareness)

다음과 관련된 보안 사항에 대한 교육을 실시할 목적으로 고용인들을 위한 프로그램이 준비되어야 한다.

- (a) 업체의 보안 정책
- (b) 보안에 대한 잠재적 내부 위협 요소 인식 능력
- (c) 화물 완전성(integrity) 유지
- (d) 접근 통제 보호
- (e) 의심 가는 화물, 인물 및 행동 인식 능력 및 보고

이러한 프로그램은 신입사원 안내 교육내용에 포함되어야 한다. 현재 위협에 대한 업데이트를 하기 위한 보습과정이 필요하다.

2.4. 면직 절차

면직된 고용인의 신원, 재산 및 정보시스템 접근 권한을 신속하게 제거하는 절차가 마련되어야 한다.

3. 사업 파트너 보안

업체들은 사업 파트너와 거래하고, 세계적 공급 체인의 보안을 향상시키기 위해 그들이 자발적으로 보안조치를 강화할 것이라는 공약을 확보해야 한다.

‘사업 파트너’(Business partner)란 업체들이 공급체인 물품을 아웃소싱 및 계약하는 상대로서 현재와 잠재적 공급자, 제조업자, 서비스 공급자, 하청업자 및 행상인들을 지칭한다.

3.1. 사업 파트너 검사

사업 파트너와의 관계를 검사, 선택, 성립시키고 재계약하는 절차가 마련되어야 한다. 절차는 인터뷰, 신원조회, 그리고 사업 파트너와 외부 공급자가 제공한 정보의 사용을 포함해야 한다. 예컨대 사업정보서비스, 은행 및 기타 기관으로부터의 기탁(referral)과 같은 것들이 있다.

다음과 같은 검사 및 선택 기준도 적용가능하다: 합법성, 재정적 지불능력과 안정성, 계약된 사항 실행 능력, 필요시 보안 결점 인식 및 개선 능력.

3.2. 협정/계약 또는 보안 선언문의 보안 조항

업체들은 서문 협정 그리고/또는 사업 파트너와의 계약상 보안 조항을 포함시키거나 사업 파트너들로 하여금 보안 선언을 제공 받아야 한다. 보안 조항 또는 선언은 어떤 방식으로 재화가 보호되며, 어떻게 관련 정보가 보호되고, 보안 보호 장치가 제시되고 제대로 설치되어 있는지 보여주어야 한다.

협정문/계약문 또는 보안 선언문은 업체들의 활동내용과 비즈니스 환경의 변화에 맞게 필요시 그리고/또는 최소한 정기적으로 이루어져야 한다.

3.3. 보안 증명서

업체들은 비즈니스 파트너의 참가에 대한 서류상의 증명서와 외국 세관 관리국, 그리고/또는 기타 보안 프로그램의 증명서를 확보해야 한다.

3.4. 비즈니스 파트너들의 보안 조치 준수 재조사

필요시에 비즈니스 파트너들의 보안 선언에 대한 유효성을 확인하기 위해 그들의 공정(processes)과 시설을 재조사해야 한다. 결과가 불만족스러울 경우 업체들은 그 사항을 비즈니스 파트너들에게 알리고, 조정을 위한 시간을 주어야 한다. 필요할 경우 업체들은 이러한 비즈니스 파트너들과의 관계를 재고할 수 있다.

4. 화물 보안

권한 받지 않은 물질 그리고/또는 인물의 침투를 막기 위해 화물 보전이 확보되어야 하며 이를 위한 절차가 갖추어져야 한다.

4.1. 문서처리 및 확인 작업

화물의 이동과 처리에 대한 전자 및 일반 문서상의 모든 정보의 읽기 용이성, 완전성, 정확성이 확보되어야 하며, 또한 정보의 교환, 손실 또는 오보의 가능성으로부터 보호할 절차가 갖추어져야 한다. 업체들은 변경, 위조 또는 기타 변칙들을 유의하여야 할 것이다.

4.2. 화물 수취 및 발송

수취되고 발송되는 화물이 관련 문서(화물 적하목록, 포장 목록, 선적 청구서구, 구매 및 배달 청구서(order))와 대조하기 위한 절차가 확보되어야 한다. 화물의 수취 및 발송시 다음의 사항이 정확한지 확인할 수 있는 절차가 확보되어야 한다. 묘사(describing), 무게확인(weighing), 상표부착, 표기, 집계, 및 확인(verify). 화물을 운송하거나 수령하는 인물들/기사들은 운송 또는 수령 전에 명확하게 신원이 확인되어야 한다.

4.3. 서명 및 날인 정책

서류 준비 절차, 봉인의 발급 및 개봉, 화물 집계, 운송기관(conveyance) 검사, 화물 운송, 수령, 그리고 미 발송 화물의 집계와 같은 *critical process handover points*²⁾와 관련된 서명 및 날인 사항을 위한 절차가 마련되어야 한다. 화물이 운송되거나 서비스가 제공될 경우 보관 및 책임과 관련된 서류는 운송 및 수취하는 인물에 의해 서명되어야 한다.

4.4. 컨테이너 검사

컨테이너 문의 잠금장치의 신뢰성을 포함하여 컨테이너의 물리적 완전성(integrity)을 확인하기 위한 절차가 확보되어야 한다. 모든 컨테이너에 대해 7가지 사항의 검사 절차가 권장된다.

- (a) 전면 벽
- (b) 좌측 면
- (c) 우측 면
- (d) 바닥

2) 적절한 번역이 어려울 경우 이탤릭체로 표시하고 밑줄을 쳤음.

- (e) 천장
- (f) 내부/ 외부 문
- (g) 외부/하부 구조(undercarriage)

4.5. 봉인 및 표기

봉인과 표기의 통제, 날인(affix), 및 확인이 어떻게 이루어질지에 대한 절차가 마련되어야 한다. 다음 조치들이 권장된다.

- (a) 오로지 지정되고 권한이 부여된 인물(들)에 의해서 봉인과 표기를 번호 매김하고 배분해야 한다.
- (b) 봉인과 표기를 받은 사원들과 그 사용처를 기록할 일지를 두어야 한다.
- (c) 번호의 예상을 방지하기 위해 봉인과 표기는 순서를 엄격하게 맞춰 번호 매김을 하면 안 된다.

컨테이너 봉인은 고(高)보안 봉인을 위한 현 PAS ISO 17712 기준을 만족시키거나 초과해야 한다.

4.6. 컨테이너 및 화물의 보관

컨테이너 및 화물은 권한 없는 접근이나 변경을 가하는 행위를 방지하기 위해 안전한 장소에서 보관되어야 한다.

4.7. 재고 통제

재고를 통제하고 화물을 보관하기 위한 절차가 마련되어야 한다. 다음의 조치들이 권장된다:

- (a) 재고 조사
- (b) 시각적으로 재고를 검사하기 위해 훈련된 감시 업체 또는 창고 직원 사용
- (c) 직원에 의해 실행되는 검사 및 재검사의 단계별 세부 항목 요구
- (d) 수취 성수기에 있어 보다 잦은 검사 및 discrepancy reporting 요구

5. 운송기관(conveyance) 보안

운송이 효과적으로 이루어질 수 있음을 확보하는 절차를 마련해야 한다.

5.1. 운송기관 검사

운송기관에 불법 재화를 은폐시킬 수 있는 잠재적 장소들을 주기적으로 확인하기 위한 절차가 마련되어야 한다. 모든 내부/외부 칸(compartment) 및 패널(panel)의 보완이 확보되어야 한다.

5.2. 운송기관(conveyance)의 추적 및 감시

업체들의 시설 내에서 그리고 업체들과 외부자들 사이의 화물 전달시 화물의 이동과 처리와 관련된 행위를 정확하게 추적하고 감시하기 위한 절차를 마련해야 한다. 추적 및 감시 시스템은 다음을 통해 실행될 수 있다:

- (a) 전자 장치. 예컨대 트랜스폰더, 스마트카드, 전자 봉인, 비디오, 디지털 사진, 휴대전화, 라디오 및 GPS; 또는
- (b) Activity logs 등

5.3. 운송업자 가이드라인

운송업자들은 수송과 화물의 상시 보안을 유지하고 지정된 보안부서 직원들에게 실제 또는 수상한 사항을 보고하도록 훈련받아야 한다. 운송업자들을 훈련하기 위한 가이드라인은 다음 사항에 관련된 것이다:

- (a) 화물의 수취(pick up) 및 운송에 대한 상세한 운송 경로 계획
- (b) 적재 하물, 경로 및 목적지의 기밀성
- (c) 열쇠, 주차 장소, 급유 및 예정되지 않은 정지(stops)
- (d) 사고 및 긴급 상황 보고
- (e) 적재, 잠금 및 봉인과 관련된 이상 발생 시 보고
- (f) 보안 경보 및 추적 장치가 있을 시 그 설치 및 시험

5.4. 운송기관의 보관

권한이 없는 접근 그리고/또는 변경을 방지하기 위해 운송기관은 안전한 장소에 보관되어야 한다.

6. 정보 및 정보기술의 보안

(일반 및 전자) 정보와 공급 체인에 사용된 정보 시스템의 기밀성 및 완전성을 보존하기 위해 정보의 오용 및 권한 없는 변경의 방지를 포함한 절차가 마련되어야 한다.

6.1. 정보 보안 정책

정보 시스템을 권한 없는 접근으로부터 보호하기 위한 정보 보안 정책과 절차 그리고/또는 방화벽, 비밀번호, 바이러스 프로그램 및 데이터 암호화 등의 보안 관련된 조정 장치가 마련되어야 한다.

6.2. 정보/문서 분류, 처리 및 접근 통제

민감성 및 중요도에 따라 정보/문서를 분류하는 절차가 마련되어야 한다. 중요하고 민감한 정보 및 문서는 권한 받은 자만 접근이 가능한 안전한 장소나 시스템 상에서 보관되어야 한다. 주어진 권리 및 특권의 적절성 및 남용 여부를 확인하기 위해 주기적인 검사가 이루어져야 한다.

6.3. 데이터 주기(life cycle) 통제

데이터의 주기를 통제하기 위한 절차가 마련되어야 한다.

6.4. 데이터 백업 및 복구 계획

정보의 손실의 방지를 위한 절차 및 백업 기능들이 마련되어야 한다.

7. 사건(incident) 관리 및 조사

사건 또는 위기 상황의 조정되고(coordinated) 구조화되었으며 포괄적인 대응을 제공하고 근본 원인에 대한 규명을 통한 재발 방지를 위한 절차를 마련해야 된다.

7.1. 사건 보고

화물의 부족 또는 과잉 공급, 비정상적 사항 또는 불법 행위 및 행정관리에 대한 보안 위반 행위와 같은 사건을 보고하기 위한 절차가 마련되어야 한다.

업체들은 사건 보고에 대한 데이터베이스를 갖추고 잠재적 보안 위협요소 및 위반행위 경향이나 유형을 감시하고 식별해야 한다.

7.2. 조사 및 분석

사건의 원인을 규명하고 재발 방지를 위한 개정 및 개선책을 실시할 목적으로 사건이 조사 및 분석되어야 하며 이를 위한 절차가 마련되어야 한다.

8. 위기 관리 및 사건 복원

사고나 보안 사건의 영향을 최소화하기 위한 위기 관리 및 복원 절차가 마련되어야 한다. 절차는 사전계획 및 이러한 특수한 상황 하에서의 운영방식에 대한 절차의 수립을 포함해야 한다.

8.1. 긴급 사태 대책(contingency or emergency plans)

사고 또는 긴급 보안 상황을 위한 긴급 사태 대책이 마련되어야 한다.

긴급 사태 대책은 해당 사항이 있는 모든 고용인들에게 전달되어야 하며 운영 및 조직상의 변화에 맞춰 주기적으로 업데이트되어야 한다. 업체들은 고용인들의 훈련 및 긴급 사태 대책의 시험을 주기적으로 실시해야 한다.

8.2. 사업 지속 계획(Business Continuity Plan- BCP)

업체들과 공급 체인에 영향을 주는 위기와 사고 당시 및 그 후에 핵심 사업 기능(Critical Business Functions-CBF)이 유지될 수 있도록 업체들은 사업 지속 계획을 마련할 것을 권장한다.

부록 2

국제 표준화기구의 사업장 경영보안 인증제도(ISO 28000)³⁾

머리말

ISO(국제표준화기구)는 국가표준화단체(ISO 회원기관)의 전 세계적인 연합체이다. 규격을 작성하는 작업은 통상적으로 ISO 기술위원회(Technical Committee)에서 담당한다. 기술위원회가 다루는 주제에 관심 있는 각 국가 회원기관은 기술위원회에서 그 나라를 대표할 권리를 갖는다. ISO와 연락관계에 있는 정부 및 비정부 국제 조직 또한 그 작업에 참여한다. ISO는 전기기술규격과 관련된 모든 작업에 대하여 IEC(국제전기 기술위원회)와 긴밀히 협력한다.

규격은 ISO/IEC Directive, Part2에 정해진 규칙에 따라 작성된 것이다.

기술위원회의 주 업무는 규격을 작성하는 것이다. 기술위원회에서 채택된 규격 초안은 투표를 위하여 회원기관에 배포된다. 초안이 규격으로 발행되기 위해서는 투표에 참여한 회원기관의 최소 75 % 이상의 찬성이 필요하다.

이 규격의 일부 내용은 특허권의 대상이 될 가능성이 있으므로 유의해야 한다. ISO는 그러한 특허권의 일부 또는 전부를 파악해야 하는 책임을 지지 않는다.

KS V ISO 28000은 공급사슬의 특정 중심점에 책임이 있는 다른 관련된 기술위원회와 협력하여 선박 및 해양 기술위원회인 ISO/TC 8에 의해 작성된 ISO 28000을 한국산업규격으로 채택한 것이다.

A. 개요

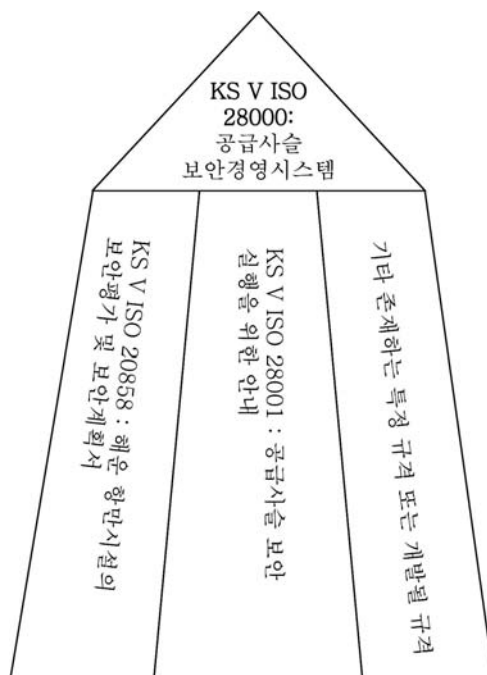
이 규격은 보안경영 규격에 대한 산업계의 요구에 부응하여 개발되었다. 이 규격의 궁극적인 목적은 공급사슬의 보안을 개선하는 것이다. 이 규격은 조직이 전체적인 공급사슬의 보안경영시스템을 수립할 수 있는 높은 수준의 경영규격이다.

3) 산업자원부 기술표준원 제공자료임

조직은 운영중인 보안환경을 평가하고 충분한 보안조치가 적소에 있는지 여부와 다른 강제적 요구사항이 조직이 준수하는 요구사항과 함께 이미 존재하는지 여부를 결정할 필요가 있다. 이 프로세스에 의해 보안 요구가 식별되었다면, 조직은 이 요구를 충족하기 위한 구조 및 프로세스를 실행하여야 한다. 공급사슬은 사실상 역동적이기 때문에, 복잡한 공급사슬을 관리하는 조직은 그림1의 설명처럼 보안 경영을 단순화하기 위하여 공급사슬에 포함되어야 할 조건인 정부 규격 또는 ISO의 공급사슬 규격을 충족하기 위해 조직의 서비스 제공자에 기대를 걸어야 할 수도 있다.

<그림 1>

KS V ISO 28000과 다른 관련 표준과의 관계



이 규격의 의도는 조직의 공급사슬이 안전한 방법으로 관리될 필요가 있는 경우에 적용되는 것이다. 보안 경영에 대한 공식 접근은 조직의 사업 능력 및 신뢰성에 직접적으로 기여할 수 있다.

규격과의 적합성이 그 자체로 법적 의무로부터의 면제를 부여 받는 것은 아니다. 그런 희망을 갖는 조직을 위하여, 보안경영시스템이 이 규격과 적합한지 여부

는 외부 또는 내부 심사 프로세스에 의해 검증될 수 있다.

이 규격은 경영시스템에 대하여 리스크를 기반으로 하는 접근방식으로 인하여 KS A ISO 14001:2004에 의해 채택된 ISO 형식에 기초한다. 그러나, 경영시스템(예; KS A ISO 9001:2007)에 프로세스 접근방식을 채택한 조직은 이 규격에서 규정한 보안경영시스템을 위한 토대로 기존 경영시스템을 사용할 수도 있다. 조직이 이미 적합성을 인증 또는 검증 받은 공급사슬 보안경영에 관한 정부의 요구사항과 규격이 중복되는 것은 이 규격의 의도가 아니다. 허용할 수 있는 1차, 2차 또는 3차 조직에 의해 검증될 수 있다.

비고 이 규격은 계획-실시-점검-조치(PDCA)로 알려져 있는 방법론에 기초하고 있다. PDCA는 다음과 같이 설명될 수 있다.

- 계획(Plan) : 조직의 보안경영방침에 따른 결과를 도출하는데 필요한 목표 및 프로세스의 수립
- 실시(Do) : 프로세스의 실행
- 점검(Check) : 보안방침, 목표, 세부목표, 법규 및 그 밖의 요구사항, 그리고 보고결과에 대한 프로세스의 모니터링 및 측정
- 조치(Act) : 보안경영시스템의 성과를 지속적으로 개선하기 위한 조치 시행

공급사슬 보안경영시스템 규격

Specification for security management systems for the supply chain

서 문

이 규격은 2007년에 제1판으로 발행된 ISO 28000 Specification for security management systems for the supply chain을 기초로 해서 기술적 내용 및 규격서의 서식을 변경하지 않고 작성한 한국산업규격이다.

A. 범위

이 규격은 공급사슬 보안보증에 필수적인 사항이 포함된 보안경영시스템에 대한 요구사항을 규정한다. 보안 경영은 기업 경영의 다른 많은 사항과 연관되어 있다. 이러한 사항에는 공급사슬 보안에 영향을 주는 조직에 의해 관리되는 또는 영향을 끼치는 모든 활동이 포함된다. 이 다른 사항은 공급사슬을 따라 상품을 운송하는 것을 포함하여 보안 경영에 영향을 주는 때와 장소에서 즉각적으로 고려되어야 한다.

이 규격은 다음 각 사항을 원하는 생산이나 공급사슬의 모든 단계에서의 제작, 서비스, 보관 또는 운송에 관계 있는, 규모가 작은 조직에서부터 다국적 기구에 이르기까지, 모든 규모의 조직에 적용 가능하다.

- (a) 보안경영시스템의 수립, 실행, 유지 및 개선
- (b) 조직이 선언한 보안경영방침과의 적합성 보증
- (c) 외부에 그러한 적합성을 실증
- (d) 공인된 제3자 인증기관에 의한 보안경영시스템의 인증/등록 추진
- (e) 이 규격에 대한 적합성을 자체 결정 및 선언

이 규격에는 몇 가지 요구사항을 언급하는 법적 및 강제적 코드가 있다.이중으

로 적합성을 실증하도록 요구하는 것이 이 규격의 의도는 아니다.

제3자 인증을 선택하는 조직은 공급사슬 보안에 현저하게 기여하고 있음을 부가적으로 실증할 수 있다.

B. 인용 규격

여기에 인용된 규격은 없다. 이 절은 다른 경영시스템 규격과 같은 번호를 유지하기 위하여 남겨 두었다.

C. 용어와 정의

이 규격의 목적을 위하여 다음과 같은 용어 및 정의를 적용한다.

a. 시설(facility)

공장, 기계, 자산, 빌딩, 차량, 선박, 항만시설 및 기반구조의 다른 항목 또는 별개의 계량 가능한 사업 기능 또는 서비스를 갖고 있는 공장 및 관련 시스템이고 이 정의는 보안의 전달 및 보안 경영을 적용하는데 필수적인 모든 소프트웨어 코드를 포함한다.

b. 보안(security)

공급사슬에 대해 또는 공급사슬에 의하여 피해 또는 손상을 주기 위하여 계획된 고의적이고 인가 받지 않은 행동에 대한 대처

c. 보안경영(security management)

조직이 조직의 리스크, 그리고 관련 있는 잠재 위협 및 그것으로부터 야기되는 영향을 최적으로 관리하는 것을 통한 체계적이고 조화된 활동 및 실행

d. 보안경영목표(security management objective)

보안 경영 방침을 충족시키기 위하여 보안과 관련하여 요구되는 구체적인 결과 또는 달성하고자 하는 것 비고 그러한 결과는 고객이나 최종 소비자에게 사업의 전체를 거쳐 나오는 제품, 공급품 또는 서비스를 제공하는 것과 직접 또는 간접으

로 연결되는 것이 필수 불가결하다.

e. 보안경영방침(security management policy)

조직의 방침 및 강제적 요구사항으로부터 도출되고 이와 일관성이 있는 보안 관련 프로세스 및 활동을 관리하기 위한 보안 및 틀과 연관된 조직의 전반적인 의도 및 방향

f. 보안경영 프로그램(programmes)

보안경영목표를 달성하는 방법

g. 보안경영 세부목표(target)

보안경영목표를 달성하기 위해 요구되는 구체적인 성과 수준

h. 이해관계자(stakeholder)

조직의 성과, 성공 또는 그 활동의 영향에 부여된 이익을 갖는 인원 또는 단체비고 예를 들어 고객, 주주, 자본가, 보험업자, 단속기관, 정부기관, 종업원, 계약자, 공급자, 노동기구 또는 사회를 포함한다.

i. 공급사슬(supply chain)

원재료 조달에서 시작하여 운송모드를 거쳐서 최종 이용자에게 상품이나 서비스 인도를 하는데 까지 확대되는 자원 및 프로세스의 연결 세트비고 공급사슬은 판매자, 제조자, 물류공급자, 내부의 배송 센터, 유통업자, 도매업자 및 최종 이용자에게 전달하는 기타 단체를 포함한다.

a) 다운스트림(downstream)

보험, 금융, 데이터 관리 및 화물의 포장, 보관 및 이송에 국한시키지 않고 다른 것도 포함하여, 화물이 조직이 직접 운영하는 관리를 떠난 후에 발생하는 공급사슬에서의 화물의 활동, 프로세스 및 움직임에 관련되는 것.

b) 업스트림(upstream)

보험, 금융, 데이터 관리 및 화물의 포장, 보관 및 이송에 국한시키지 않고 다른

것도 포함하여, 화물이 조직이 직접 운영하는 관리를 받기 전에 발생하는 공급사슬에서의 화물의 활동, 프로세스 및 움직임에 관련되는 것.

j. 최고경영자(top management)

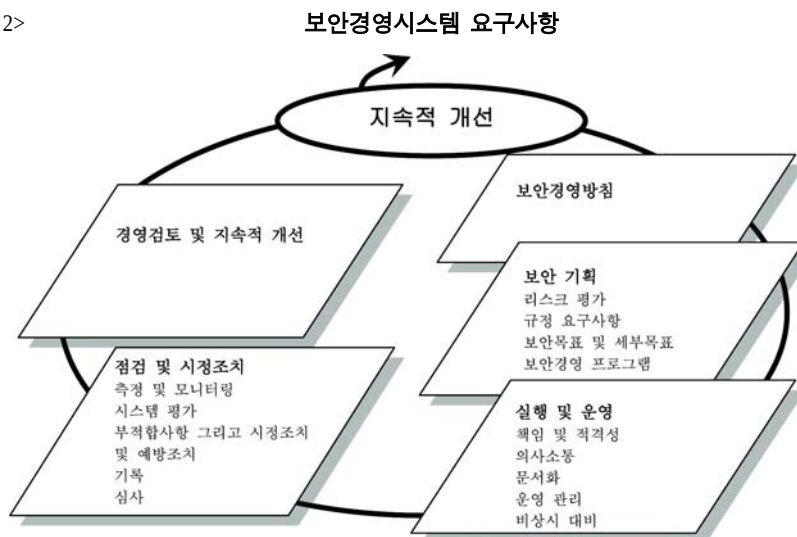
최고의 위치에서 조직을 지휘하고 관리하는 사람 또는 집단이고 최고 경영자는, 특히 대형 다국적 조직에서는, 이 규격에 서술된 바와 같이 개인적으로 관여되지 않을 수도 있다. 그러나 지휘망을 통하여 최고 경영자의 책임은 증명되어야 한다.

k. 지속적 개선(continual improvement)

조직의 보안 방침과 일관성이 있는 전반적인 보안성과의 개선을 달성하기 위해 보안경영시스템의 증진을 반복하는 프로세스

D. 보안경영시스템 요구사항

<그림 2>



a. 일반 요구사항

조직은 보안 위협을 식별하고, 리스크를 평가하여 관리하며 심각성을 경감시키기 위한 효과적인 보안경영시스템을 수립, 문서화, 실행, 유지 및 지속적으로 개선

하여야 한다.

조직은 4항 전체에 설정되어 있는 요구사항에 따라 그 효과성을 지속적으로 개선하여야 한다.

조직은 조직의 보안경영시스템의 적용범위를 규정하여야 한다. 조직이 이 요구사항에 대한 적합성에 영향을 미치는 어떤 프로세스를 외주처리 할 경우, 조직은 이러한 프로세스가 관리된다는 것을 보장해야 한다. 이러한 외주 프로세스에 대하여 필요한 관리와 책임은 보안경영시스템 내에서 파악되어야 한다.

b. 보안경영방침

조직의 최고경영자는 전반적인 보안경영방침을 승인하여야 한다. 이 방침은 다음과 같아야 한다.

- (a) 조직의 다른 방침과 일관성이 있을 것
- (b) 구체적인 보안경영 목표, 세부목표 및 프로그램을 도출할 수 있는 틀을 제공할 것.
- (c) 조직의 전반적인 보안 위협 및 리스크 관리(management) 틀과 일관성이 있을 것.
- (d) 조직에 대한 위협과 조직 운영의 특성 및 규모에 적합할 것.
- (e) 전반적인/포괄적인 보안 경영 목표를 명확하게 기술할 것.
- (f) 보안 경영 프로세스의 지속적인 개선 의지를 포함할 것.
- (g) 현재 적용되는 법규, 강제적 및 법적 요구사항과 조직이 동의한 그 밖의 요구사항을 준수하겠다는 의지를 포함할 것
- (h) 최고경영자의 승인이 명확할 것
- (i) 문서화되어 실행되고 유지될 것
- (j) 모든 관련된 종업원 및 계약자와 방문자를 포함한 제3자가 각자의 보안경영 관련 의무사항을 인지할 수 있도록 의사소통 될 것
- (k) 필요한 경우 이해관계자가 이용할 수 있도록 할 것
- (l) 보안 경영 시스템의 연속성 및 관련성에 영향을 줄 수 있는 다른 조직과의 인수 또는 합병, 또는 조직의 사업범위가 변경되는 경우 보안경영방침이 검토되도록 할 것.

비고

조직이 보안경영시스템을 운영하기 위하여 충분한 정보 및 지시를 제공하는 내부목적으로 상세한 보안경영방침을 선택할 수 있고(일부는 사외비로 할 수 있음) 조직의 이해관계자와 기타 이해관계자에게 배포하기 위하여 개략적인 목표를 나타내는 요약본(공개용)을 선택할 수 있다.

c. 보안리스크 평가 및 기획

a) 보안리스크 평가

조직은 보안 위협뿐만 아니라 보안 경영 관련 위협 및 리스크를 지속적으로 식별 및 평가하고, 필요한 경영 관리 수단을 식별 및 실행하기 위한 절차를 수립하고 유지하여야 한다. 보안 위협 및 리스크의 식별, 평가 및 관리 방법은, 최소한, 운영 특성 및 규모에 적합하여야 한다. 이러한 평가는 일(event)의 발생 가능성과 그것으로 인한 모든 결과를 반드시 고려하여야 하며 다음을 포함하여야 한다.

- (a) 기능상의 실패, 우발적 손상, 의도적인 손상, 또는 테러리스트나 범죄 행위 등과 같은 물리적인 실패 위협 및 리스크
- (b) 조직의 성과, 상황 또는 안전에 영향을 미치는 보안 관리, 인적요소 및 기타 활동을 포함하는 운영상의 위협 및 리스크
- (c) 보안 조치 및 장비를 무력하게 만들 수 있는 자연환경적 일 (폭우, 홍수, 기타)
- (d) 외부에서 제공된 장비 및 서비스에서의 실패와 같은 조직의 관리를 벗어나는 요소
- (e) 법적 요구사항 불이행 및 조직의 명성 또는 브랜드의 손상과 같은 이해관계자의 위협 및 리스크
- (f) 보안 장비의 설계 및 설치 (대체, 정비 및 기타의 경우를 포함)
- (g) 정보 및 데이터 관리와 의사소통
- (h) 운영 지속성에 대한 위협

조직은 이러한 평가의 결과 및 관리의 효과를 고려하고 적절한 경우 다음 항목의 입력 자료로 활용됨을 보장하여야 한다.

- (a) 보안 경영 목표 및 세부목표
- (b) 보안 경영 프로그램
- (c) 설계, 규격 및 설치의 요구사항에 대한 결정

- (d) 직원의 수준을 포함하는 적절한 자원의 식별
- (e) 교육훈련 필요성 및 숙련도의 식별 (4.4.2 참조)
- (f) 운영 관리의 개발 (4.4.6 참조)
- (g) 조직의 전반적인 위협 및 리스크 관리 틀

조직은 이러한 정보를 문서화하고 최신의 것으로 유지하여야 한다.

위협 및 리스크를 식별하고 평가하기 위한 방법은 다음과 같은 조건을 만족해야 한다.

- (a) 사후적이지 않고 사전적으로 되도록 적용범위, 특성 및 시점을 고려하여 규정될 것
- (b) 보안 위협 및 리스크와 관련된 정보의 수집을 포함할 것
- (c) 회피하고, 제거되거나 관리될 수 있도록 위협 및 리스크의 분류와 그것의 식별을 제공할 것
- (d) 실행의 효과성 및 시의 적절성 모두를 보장하기 위한 조치에 대해 모니터링 할 수 있도록 할 것(4.5.1 참조)

b) 법률, 강제 요구사항 및 그 밖의 보안규정 요구사항

조직은 다음의 절차를 수립, 실행 및 유지하여야 한다.

- (a) 조직의 보안 위협 및 리스크와 관련하여 적용되는 법적 요구사항 및 조직이 준수하기로 한 기타 요구사항을 식별하고 입수하는 것
 - (b) 이러한 요구사항이 보안 위협 및 리스크에 어떻게 적용되는지를 결정하는 것
- 조직은 이러한 정보를 최신의 것으로 유지하여야 한다. 법률 및 그 밖의 요구사항에 관한 정보는 조직의 종업원과 계약자를 포함하여 그 밖의 관련된 제3자와 의사소통 하여야 한다.

c) 보안경영목표

조직은 내부의 관련 기능 및 계층별로 문서화된 보안경영목표를 수립, 실행 및 유지하여야 한다. 이 목표는 방침으로부터 나와야 되며 방침과 일관성이 있어야 한다. 조직이 목표를 수립하고 검토할 때에는 다음 사항을 고려하여야 한다.

- (a) 법률, 법적 및 그 밖의 보안에 관련된 강제적 요구사항
- (b) 보안과 관련된 위협 및 리스크
- (c) 기술적 및 그 밖의 선택사항

(d) 재정적, 운영적 및 사업상의 요구사항

(e) 적절한 이해관계자의 견해.

보안경영목표는 다음과 같아야 한다.

(a) 조직의 지속적인 개선 의지와 일관성이 있을 것

(b) 계량화 할 것(실행 가능한 경우)

(c) 모든 관련된 종업원 및 계약자를 포함한 제3자가 각 개인의 의무사항을 인지할 수 있도록 의사소통 될 것

(d) 보안경영방침과의 연관성 및 일관성을 유지하도록 보장하기 위하여 주기적으로 검토할 것. 그에 따라서 필요한 경우 보안 경영 목표를 수정할 것.

d) 보안경영 세부목표(target)

조직은 조직의 요구에 적절하고 문서화된 보안경영세부목표를 수립, 실행 및 유지하여야 한다. 이 세부목표는 보안경영목표로부터 도출되어야 하며 보안경영목표와 일관성이 있어야 한다.

이 세부목표는 다음과 같아야 한다.

(a) 적절하게 상세할 것

(b) 구체적이고, 측정가능하고, 달성가능하고, 관련성 및 시간 기준이 있을 것 (실행 가능한 경우)

(c) 모든 관련된 종업원 및 계약자를 포함한 제3자가 각 개인의 의무사항을 인지할 수 있도록 의사소통 될 것

(d) 보안경영목표와의 연관성 및 일관성을 유지하도록 보장하기 위하여 주기적으로 검토할 것. 그에 따라서 필요한 경우 보안경영 세부목표를 수정할 것

e) 보안경영 프로그램(programmes)

조직은 조직의 목표 및 세부목표를 달성하기 위한 보안경영 프로그램을 수립, 실행 및 유지하여야 한다.

프로그램은 최적화되고 우선순위가 결정되어야 하며, 조직은 프로그램을 효율적이고 비용 효과적으로 실행하여야 한다.

프로그램에는 다음 사항을 기술하여 문서화하여야 한다.

(a) 보안경영목표 및 세부목표를 달성하기 위하여 부여된 책임 및 권한

(b) 보안경영목표 및 세부목표를 달성하기 위한 수단 및 일정

보안경영 프로그램은 목표 및 세부목표와의 효과성 및 일관성을 유지하도록 보장하기 위하여 주기적으로 검토되어야 한다. 그에 따라서 필요한 경우 프로그램은 수정되어야 한다.

d. 실행 및 운영

a) 보안 경영의 구조, 권한 및 책임

조직은 보안경영 방침, 목표, 세부목표 및 프로그램의 달성과 일관성이 있게 역할, 책임 및 권한에 대한 조직 구조를 수립하고 유지하여야 한다.

이러한 역할, 책임 및 권한은 규정되고, 문서화되어 실행 및 유지에 책임이 있는 각 개인과 의사소통 되어야 한다.

최고경영자는 보안경영시스템(프로세스)의 개발 및 실행과 그것의 지속적인 효과성 개선에 대한 의지의 증거를 다음과 같이 나타내어야 한다.

- (a) 다른 책임과는 무관하게 조직의 보안 경영 시스템의 전반적인 설계, 유지, 문서화 및 개선에 대한 책임이 있는 최고 경영자의 인원을 지정
- (b) 목표 및 세부목표가 실행되고 있음을 보장하기 위하여 필요한 권한을 가진 관리자(1인 또는 다수)를 지정
- (c) 조직의 이해관계자의 요구사항 및 기대를 점검하고 모니터링하며 이 기대를 관리하기 위한 적절하고 시기 적절한 조치를 시행
- (d) 충분한 자원의 가용성을 보장
- (e) 보안 경영 방침, 목표, 세부목표, 프로그램 등이 조직의 다른 사항에 미칠 수 있는 부정적 영향도 고려
- (f) 조직의 다른 부분에서 생성된 어떠한 보안 프로그램도 보안경영 시스템을 보완하도록 보장할 것
- (g) 조직의 방침에 적합하기 위해서는 조직의 보안경영 요구사항을 충족시키는 것이 중요하다는 것에 대하여 조직과 의사소통 할 것
- (h) 보안 관련 위협 및 리스크가 평가되고 이것이 조직의 위협 및 리스크 평가에 적절히 포함됨을 보장
- (i) 보안경영 목표, 세부목표 및 프로그램의 실행 가능성을 보장

b) 적격성, 교육훈련 및 인식

조직은 보안 장비 및 프로세스를 설계, 운영 및 관리할 책임이 있는 인원이 학력, 훈련 및/또는 경험에 따라 적절한 자격이 있음을 보장하여야 한다. 조직은 조직에 근무하는 종업원이나 조직을 대신하여 업무를 실행하는 인원에게 다음 사항을 인식시키기 위한 절차를 수립하고 유지하여야 한다.

- (a) 보안경영방침 및 절차 그리고 보안경영시스템 요구사항과의 적합성에 대한 중요성
- (b) 비상시 대비 및 대응 요구사항을 포함하여 보안경영방침 및 절차 그리고 보안경영시스템 요구사항에 적합하기 위하여 필요한 역할 및 책임
- (c) 규정된 운영 절차로부터 벗어남으로 인해 조직의 보안에 미치는 잠재적 결과

적격성 및 교육훈련 기록은 유지되어야 한다.

c) 의사소통

조직은 관련 보안 경영 정보가 관련된 종업원, 계약자 및 그 밖의 이해관계자와 의사소통 되는 것을 보장하기 위한 절차를 가지고 있어야 한다.

특정한 보안 관련 정보는 민감한 특성이 있으므로 배포 전에 정보의 민감성을 고려하여야 한다.

d) 문서화

조직은 다음 사항을 포함하는 보안 경영 문서화 시스템을 수립하고 유지해야 한다. 그러나 반드시 다음 사항에 국한되지는 않는다.

- (a) 보안 방침, 목표 및 세부목표
- (b) 보안경영시스템 범위에 대한 기술
- (c) 보안경영시스템의 주요 요소 및 그의 상호작용과 관련 문서와의 관계에 대한 기술
- (d) 기록을 포함하여 이 규격에서 요구하는 문서
- (e) 기록을 포함하여, 중요한 보안 위협 및 리스크와 관련된 프로세스를 효과적으로 계획, 운영 및 관리하는 것을 보장하기 위하여 필요하다고 조직이 결정한 문서

조직은 정보의 보안 민감도를 결정하고 비인가자의 접근을 방지할 수 있는 조치를 취해야 한다.

e) 문서 및 데이터 관리

조직은 다음 사항을 보장하기 위하여 이 규격의 4항에서 요구하는 모든 문서, 데이터 및 정보를 관리하기 위한 절차를 수립하고 유지하여야 한다.

- (a) 이러한 문서, 데이터 및 정보는 적절한 장소에 비치되고 권한을 가진 자만이 접근
- (b) 이러한 문서, 데이터 및 정보는 주기적으로 검토하고, 필요에 따라 개정하며, 권한을 가진 자가 그 적절성을 승인
- (c) 보안경영시스템의 효과적인 기능 발휘에 필수적인 업무를 수행하는 모든 장소에서 관련 문서, 데이터 및 정보의 최신판을 이용할 수 있어야 함.
- (d) 효력이 상실된 문서, 데이터 및 정보는 모든 발행 장소 및 사용 장소에서 신속히 제거되거나, 달리 사용되지 않음을 보장하여야 함.
- (e) 법률에 의하여 또는 지식 보존의 목적으로 보유하고 있는 문서, 데이터 및 정보는 적절하게 식별되어야 함.
- (f) 이러한 문서, 데이터 및 정보는 안전하게 보관하여야 하며, 전자화된 형태인 경우 적절하게 백업하고 복구할 수 있어야 함.

f) 운영 관리

조직은 다음을 달성하는데 필요한 운영 및 활동을 파악하여야 한다.

- (a) 조직의 보안 경영 방침
- (b) 중대한 리스크를 가지고 있다고 식별된 위협의 감소 및 활동의 관리
- (c) 법률, 법적 및 그 밖의 강제적 요구사항에 대한 적합성
- (d) 조직의 보안경영목표
- (e) 조직의 보안경영 프로그램의 실행
- (f) 공급사슬 보안에서 요구되는 수준

조직은 다음 사항에 따라 규정된 조건 하에 이러한 운영 및 활동이 수행되고 있음을 보장하여야 한다.

- (a) 문서화된 절차가 없음으로 인하여 4.4.6 a)에서 f)까지 나열된 운영 및 활동을 달성하지 못하는 상황이 발생하는 것을 관리하기 위해 문서화된 절차

를 수립, 실행 및 유지

- (b) 업스트림 공급사슬 활동으로 야기되는 위협을 평가하고 조직 및 그 밖의 다운스트림 공급사슬 운영자에 대한 이 영향을 경감시키기 위한 관리를 적용

- (c) 보안에 영향을 주는 상품 및 서비스에 대한 요구사항을 수립 및 유지하고, 이를 공급자 및 계약자와 의사소통 함

이러한 절차는 적용 가능한 경우 장비, 도구 등에 대한 보안 관련 항목의 설계, 설치, 운영, 개조 및 변경에 대한 관리를 포함하여야 한다. 현재의 제도가 개정되거나 새로운 제도가 도입되어 보안 경영 운영 및 활동에 영향을 줄 수 있는 경우 조직은 그 제도의 실행 이전에 관련된 보안 위협 및 리스크를 고려하여야 한다. 제정 또는 개정되는 제도는 다음 사항을 반드시 고려하여야 한다.

- (a) 개정되는 조직의 구성, 역할 또는 책임
- (b) 개정되는 보안경영 방침, 목표, 세부목표 또는 프로그램
- (c) 개정되는 프로세스 및 절차
- (d) 하드웨어 및/또는 소프트웨어를 포함하여 새로운 기반구조, 보안 장비 또는 기술의 소개
- (e) 해당되는 경우, 신규 계약자, 공급자 또는 인원의 소개

g) 비상시 대비, 대응 및 보안 복구

조직은 보안사건 및 비상사태의 잠재적 발생 가능성을 파악하고 이에 대한 대응, 그리고 이러한 상황과 관련하여 일어날 수 있는 심각성을 방지하고 완화시키기 위한 적절한 계획 및 절차를 수립, 이행 및 유지하여야 한다. 이 계획 및 절차는 사건 또는 비상사태 중에 또는 이후에 요구될 수 있는 모든 식별된 장비, 시설 또는 서비스의 공급 및 정비에 관한 정보를 포함하여야 한다.

조직은 비상시 대비, 대응 및 보안 복구 계획과 절차의 효과성을 주기적으로 검토하여야 하며 특히 보안 위반 및 위협으로 인해 야기된 사건 또는 비상사태가 발생한 이후에는 반드시 그러하여야 한다. 조직은 이러한 절차를 실행 가능한 방법으로 주기적으로 시험하여야 한다.

e. 점검 및 시정조치

a) 보안성과 측정 및 모니터링

조직은 보안 경영 시스템의 성과를 모니터링하고 측정할 수 있는 절차를 수립 및 유지하여야 한다. 또한 보안성과를 모니터링하고 측정할 수 있는 절차도 수립하여야 한다. 조직은 주요 성과 요소를 측정하고 모니터링하기 위한 주기를 정할 때 잠재적인 악화 구조(deterioration mechanism) 및 그 심각성을 포함하여 관련된 보안 위협 및 리스크를 고려하여야 한다. 이 절차는 다음 사항을 제공하여야 한다.

- (a) 조직의 필요성에 적절한 정성적 및 정량적 측정
- (b) 조직의 보안경영 방침, 목표 및 세부목표를 어느 정도까지 충족시켰는지를 모니터링
- (c) 보안경영 프로그램, 운영 관리 기준 및 적용 가능한 법률, 법적 요구사항 및 그 밖의 보안관련 강제적 요구사항의 적합성을 모니터링하기 위한 능동적인 성과 측정
- (d) 보안 관련 악화, 실패, 사건, 부적합사항(준사고(near miss) 및 오경보를 포함한) 및 기타 보안경영시스템의 성과 저하 이력을 모니터링하기 위한 반응적 성과 측정
- (e) 사후의 시정조치 및 예방조치의 분석을 용이하게 하기 위해 충분한 모니터링 및 측정의 데이터와 결과를 기록. 성과 및/또는 측정과 모니터링에 모니터링 장치가 필요하다면, 조직은 이러한 장치의 교정 및 정비 활동을 위한 절차를 수립하고 유지하여야 한다. 교정 및 정비 활동과 결과의 기록은 법규 및 조직의 방침을 준수하기 위해 충분한 기간 동안 보존되어야 한다.

b) 시스템 평가

조직은 주기적인 검토, 시험, 사건 후 보고서, 교훈, 성과 평가 및 연습을 통해 보안 경영 계획, 절차 및 능력을 평가하여야 한다. 이러한 요소의 주요 변경 사항은 즉시 절차에 반영되어야 한다.

조직은 관련 법규 및 강제 요구사항, 산업계 우수 관행에 대한 적합성 여부, 그리고 조직의 방침 및 목표에 대한 적합성을 주기적으로 평가하여야 한다.

조직은 주기적 평가의 결과에 대한 기록을 유지하여야 한다.

c) 보안 관련 실패, 사건, 부적합사항 그리고 시정조치 및 예방조치

조직은 다음과 같은 사항에 대한 책임 및 권한을 규정하는 절차를 수립, 실행 및 유지해야 한다.

- (a) 발생을 방지할 수 있도록 보안의 잠재 실패를 식별하기 위한 예방 조치의 평가 및 착수
- (b) 다음과 같은 보안 관련 사항의 조사
 - (1) 준사고 및 오정보를 포함하는 실패
 - (2) 사건 및 비상 사태
 - (3) 부적합사항
- (c) 이러한 실패, 사건 또는 부적합사항으로 인해 발생하는 모든 심각성을 경감시키기 위한 조치의 수행
- (d) 시정 조치의 착수 및 완료
- (e) 취해진 시정 조치의 효과성 확인

이러한 절차는 즉각적인 실행이 생명 또는 공공 안전에 대한 절박한 노출을 사전에 막는 것이 아니라면 모든 제안된 시정조치 및 예방조치가 실행 전에 보안 위협 및 리스크 평가 프로세스를 통하여 검토되도록 요구해야 한다.

실제적 및 잠재적 부적합사항의 원인을 제거하기 위한 모든 시정조치 또는 예방조치는 문제점의 크기에 적절하여야 하고 직면할 수 있는 보안 경영 관련 위협 및 리스크에 적절한 것이어야 한다. 조직은 시정조치 및 예방조치의 결과로 인한 문서화된 절차의 모든 변경을 실행하고 기록하여야 하며, 필요한 경우 요구된 교육훈련을 포함시켜야 한다.

d) 기록관리

조직은 보안경영 시스템 및 이 규격의 요구사항에 대한 적합성과 달성된 결과를 실증하기 위해 필요한 기록을 작성하고 유지하여야 한다.

조직은 기록의 식별, 보관, 보호, 검색, 보유 및 폐기에 대한 절차를 수립, 실행 및 유지하여야 한다.

기록은 읽기 쉽고, 식별 및 추적이 가능해야 한다.

전자 및 디지털 문서는 기록 조작을 방지할 수 있고 안전하게 백업되고 인가자만이 접근할 수 있어야 한다.

e) 심사

조직은 보안경영 심사 프로그램(program)을 수립, 실행 및 유지하여야 하고, 다음을 위한 보안경영 시스템에 대한 심사가 계획된 주기에 따라 수행됨을 보장하여야 한다.

- (a) 보안 경영 시스템이 다음 사항을 만족하는지의 결정
 - (1) 이 규격 4항의 전체 요구사항을 포함하여 보안 경영을 위해 계획된 결정 사항에 적합함
 - (2) 적절하게 실행되고 유지됨
 - (3) 조직의 보안경영 방침 및 목표를 효과적으로 충족시키고 있음
- (b) 이전의 심사 결과 및 부적합사항을 시정하기 위한 조치를 검토c) 경영자에게 심사 결과에 대한 정보를 제공
- (d) 보안 장비 및 인원이 적절하게 배치되었는지를 검증모든 일정을 포함하여, 심사 프로그램은 조직 활동에 대한 위협 및 리스크 평가 결과와 이전의 심사 결과에 근거하여야 한다. 심사 절차에는 심사의 수행 및 결과 보고에 대한 책임 및 요구사항 뿐만 아니라, 적용 범위, 주기, 방법 및 적격성이 포함되어야 한다. 가능한 한 심사는 점검이 이루어지는 활동에 직접적인 책임이 없는 사람에 의해 수행되어야 한다.비고 “책임이 없는 사람”이라고 해서 반드시 조직의 외부 인원을 의미하는 것은 아니다.

f. 경영검토 및 지속적 개선

최고경영자는 지속적인 적절성, 충족성 및 효과성을 보장하기 위하여 계획된 주기로 보안경영시스템을 검토하여야 한다. 이 검토에는 개선을 위한 기회 평가 그리고 보안방침, 보안목표 그리고 위협 및 리스크를 포함한 보안경영시스템에 대한 변경 필요성을 포함하여야 한다. 경영검토의 기록은 보유되어야 한다.

경영검토의 입력사항에는 다음을 포함하여야 한다.

- (a) 법규 요구사항과 조직이 동의한 그 밖의 요구사항에 대한 적합성 심사 및 평가의 결과
- (b) 불만사항을 포함하여 외부 이해관계자와의 의사소통
- (c) 조직의 보안성과
- (d) 목표 및 세부목표 달성정도

- (e) 시정조치 및 예방조치의 상태
- (f) 이전 경영검토의 후속 조치
- (g) 조직의 보안사항과 관련된 법규 및 기타 요구사항의 개발을 포함하여 변화하는 주변여건
- (h) 개선을 위한 제안

경영검토의 출력에는 지속적 개선에 대한 의지와 일관성이 있도록 보안방침, 목표 및 보안경영시스템의 기타 요소의 가능한 변경에 관련된 결정과 조치를 포함하여야 한다.

부속서A

(참고)

KS V ISO 28000 : 2007, KS A ISO 14001 : 2004 및 KS A ISO 9001 : 2007의 대비표

KS V ISO 28000:2007		KS A ISO 14001:2004		KS A ISO 9001:2007	
공급사슬 보안경영시스템 요구사항 (제목만)	4	환경경영시스템 요구사항 (제목만)	4	품질경영시스템 요구사항 (제목만)	4
일반 요구사항	4.1	일반 요구사항	4.1	일반 요구사항	4.1
보안경영방침	4.2	환경 방침	4.2	경영 의지 품질 방침 지속적 개선	5.1 5.3 8.5.1
보안 리스크 평가 및 기획 (제목만)	4.3	기획 (제목만)	4.3	기획 (제목만)	5.4
보안 리스크 평가	4.3.1	환경측면	4.3.1	고객중심 제품과 관련된 요구사항 결정 제품과 관련된 요구사항 검토	5.2 7.2.1 7.2.2
법률, 강제 요구사항 및 그 밖의 보안규정 요구사항	4.3.2	법규 및 그 밖의 요구사항	4.3.2	고객중심 제품과 관련된 요구사항 결정	5.2 7.2.1
보안경영목표	4.3.3	목표, 세부목표 및 추진계획	4.3.3	품질목표 품질경영시스템 기획 지속적 개선	5.4.1 5.4.2 8.5.1
보안경영 세부목표	4.3.4	목표, 세부목표 및 추진계획	4.3.3	품질목표 품질경영시스템 기획 지속적 개선	5.4.1 5.4.2 8.5.1
보안경영 프로그램	4.3.5	목표, 세부목표 및 추진계획	4.3.3	품질목표 품질경영시스템 기획 지속적 개선	5.4.1 5.4.2 8.5.1
실행 및 운영 (제목만)	4.4	실행 및 운영 (제목만)	4.4	제품실행 (제목만)	7
보안경영의 구조, 권한 및 책임	4.4.1	자원, 역할, 책임 및 권한	4.4.1	경영의지 책임 및 권한 경영대리인 자원확보 기반구조	5.1 5.5.1 5.5.2 6.1 6.3
적격성, 교육훈련 및 인식	4.4.2	적격성, 교육훈련 및 인식	4.4.2	(인적자원) 일반 사항 적격성, 교육훈련 및 인식	6.2.1 6.2.2

KS V ISO 28000:2007		KS A ISO 14001:2004		KS A ISO 9001:2007	
의사소통	4.4.3	의사소통	4.4.3	내부 의사소통 고객과의 의사소통	5.5.3 7.2.3
문서화	4.4.4	문서화	4.4.4	(문서화 요구사항) 일반 사항	4.2.1
문서 및 데이터 관리	4.4.5	문서 관리	4.4.5	문서 관리	4.2.3
운영 관리	4.4.6	운영 관리	4.4.6	제품실현의 기획 제품과 관련된 요구사항의 결정 제품과 관련된 요구사항의 검토 설계 및 개발 기획 설계 및 개발 입력 설계 및 개발 출력 설계 및 개발 검토 설계 및 개발 검증 설계 및 개발 타당성 확인 설계 및 개발 변경 관리 구매프로세스 구매정보 구매한 제품의 검증 생산 및 서비스 제공의 관리 생산 및 서비스 제공에 대한 프로세스의 타당성 확인 제품의 보존	7.1 7.2.1 7.2.2 7.3.1 7.3.2 7.3.3 7.3.4 7.3.5 7.3.6 7.3.7 7.4.1 7.4.2 7.4.3 7.5.1 7.5.2 7.5.5
비상시 대비, 대응 및 보안 복구	4.4.7	비상사태 대비 및 대응	4.4.7	부적합제품의 관리	8.3
점검 및 시정조치 (제목만)	4.5	점검 (제목만)	4.5	측정, 분석 및 개선 (제목만)	8
보안 성과 측정 및 모니터링	4.5.1	모니터링 및 측정	4.5.1	모니터링장치 및 측정장치의 관리 일반 사항(측정, 분석 및 개선) 프로세스의 모니터링 및 측정 제품의 모니터링 및 측정 데이터의 분석	7.6 8.1 8.2.3 8.2.4 8.4
시스템 평가	4.5.2	준수평가	4.5.2	프로세스의 모니터링 및 측정 제품의 모니터링 및 측정	8.2.3 8.2.4

KS V ISO 28000:2007		KS A ISO 14001:2004		KS A ISO 9001:2007	
보안관련 실패, 사건, 부적합 사항, 그리고, 시정조치 및 예방조치	4.5.3	부적합, 시정조치 및 예방조치	4.5.3	부적합 제품의관리 데이터의 분석 시정조치 예방조치	8.3 8.4 8.5.2 8.5.3
기록관리	4.5.4	기록관리	4.5.4	기록관리	4.2.4
심사	4.5.5	내부심사	4.5.5	내부심사	8.2.2
경영검토 및 지속적 개선	4.6	경영검토	4.6	경영의지 경영검토 (제목만) 일반사항 검토입력 검토출력 지속적 개선	5.1 5.6 5.6.1 5.6.2 5.6.3 8.5.1

국가 물류보안체제 확립방안 연구(Ⅱ)

2007年 12月 27日 印刷
2007年 12月 31日 發行

編輯兼 發行人	李 正 煥
發行處	韓國海洋水產開發院 서울특별시 서초구 방배3동 1027-4
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