물류학석사 학위논문

해운기업의 해상공급사슬보안과 위험관리전략에 관한 연구

A Study on the Maritime Supply Chain Security and Risk Management Strategies of Shipping Industry

지도교수 신 영 란

2019년 2월

한국해양대학교 글로벌물류대학원

해 운 항 만 물 류 학 과

권 유 성

본 논문을 권유성의 물류학석사 학위논문으로 인준함.

위원장 김 율 성 ㊞

위 원 김 강 혁 ㊞

위 원 신 영 란 ㊞

2018년 12월

한 국 해 양 대 학 교 글 로 벌 물 류 대 학 원

< 목 차 >

<표 목차>

<그림 목차>

국문초록

해운기업의 해상공급사슬보안과 위험관리전략에 관한 연구

권 유 성
글로벌물류대학원 해운항만물류학과

최근 선진국과 국제무역기구의 동향에 따르면 911테러 이후 국제 사회의 주요 이슈로 공항과 항만 등을 비롯하여 국제물류 전 단계에서의 보안과 효율성 강화, WCO, 미국, EU가 주도하는 무역안전망 확보를 위한 국제물류보안체제 구축이 적극 추진되고 있다.

본 연구에서는 선박보안사고의 현황과 원인을 파악하여 선박보안관리의 특성을 조사하고 선박보안관리시스템의 취약점을 분석하였다. 또한 해상공급사슬보안의 개념과 특징, 보안위험과 공급사슬의 취약성을 조사하였다.

국제기구의 해상공급사슬보안제도 및 주요국의 해상공급사슬보안 인증제도 현황을 분석하여 해상공급사슬보안의 문제점을 개선하고, 모든 물류 구역에서 발생할 수 있는 테러 공격과 같은 보안 사고를 예방함으로써 해상공급사슬이 실시간으로 원활히 운영되도록 유도하였다.

또한, 해운회사의 해상공급사슬보안 요소 및 범위를 확립하고, 보안위험을 예방하고 위험성을 감소하기 위하여 수립된 대책 등 관련 자료를 수집하였다.

이를 통해 유형별 해상보안위험에 효과적으로 대처할 수 있는 보안체계 구축 방법과 해운회사의 해상공급사슬 보안사고 예방을 위한 효과적인 리스크 관리전략을 제안하였다.

Abstract

A Study on the Maritime Supply Chain Security and Risk Management Strategies of Shipping Industry

Kwon, Yu Sung

Department of Shipping and Port Logistics
Graduate School of Global Logistics

According to the recent trend of advanced countries and international trade organizations, the strengthening of security and efficiency of international logistics such as airports and seaports has emerged as a major issue in the international community after 9.11 terrorist attacks, and the establishment of an international logistics security system has been actively promoted to secure trade safety net led by WCO, U.S. and EU.

In this study, the status and cause of ship security accidents were identified to examine the characteristics of ship security management and to analyze the vulnerability of the ship security management system.

The concepts and characteristics of maritime supply chain security, security risk and vulnerabilities in the supply chain were researched.

Further, the current status of the maritime supply chain security system of international organizations and the maritime supply chain security certification

system of major countries were analyzed and derived implications to ensure that the logistics security system is operated in real time by improving problems in maritime supply chain security and preventing security accidents such as possible terror attacks in all logistics sections.

In addition, related data were collected to establish maritime supply chain security elements and scope of the shipping companies, and establish measures to prevent security risks and reduce risks of the shipping companies.

Through this, effective risk management strategies for security accidents of shipping companies are proposed by establishing a personal and physical security system to effectively cope with each type of maritime security risk.

제1장 서 론

인류가 해상활동을 시작한 이래로 해상에서의 인적, 물적 재해를 예방하기 위한 노력은 계속되고 있다. 초기에 해상에서의 안전 확보는 교육과 훈련을 통한 선박 운항자의 자질향상에 집중되었으나, 과학 기술 발달에 의해 신뢰성이 보장된 안전 장비 개발과 혁신적인 통신기술 도입, 선박 간의 협조와 육상에서의 지원까지 가능해짐으로써 해상의 안전도는 더욱 향상되고 있다. 이와 더불어 해상에서의 인명과 재산, 환경을 보호하고 안전에 대한 요구에 부응하기 위한 해양안전정책의 수립으로 국내외 해난사고는 꾸준히 감소하고 있다.

국제해사기구는 해상테러를 방지하기 위하여 2001년 총회에서 채택한 결의서에 따라 해상 테러를 방지하기 위한 대책을 마련하였다. 총회 결의서는 해상항해 안전에 대한 불법행위 억제에 관한 협약(Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988; SUA협약) 후의 개정 필요성에 대한 검토와 해상테러 방지 조치시 다른 안전 관련 국제기구의 경우를 참고할 것을 권고하였다. 그리고 1998년 SUA 협약과 그 의정서를 채택하지 않은 국가는 조속히 합류할 것을 당부하였다. 또한, 각국의 항만과 터미널 등에 적절한 안전조치를 갖추고, 사무총장은 테러 방지를 위해 항만의 안전과 안보 강화에 힘쓰는 회원국을 지원하도록 명시하였다.

2002년 IMO 법률위원회의 제84차 회의에서는 해상테러 방지대책에 대하여 집중적으로 논의되었다. 미국은 유해물질을 사용하는 행위 및 선박을 무기로 사용하는 행위 등을 불법행위로 규정하고, 정치범죄에 대한 예외 조항 배제와 범죄인의 타국인도 등에 관한 규정을 추가할 필요성에 대하여 주장하였다. 터키는 해상테러 방지협약으로 협약의 명칭을 개정하고, UN 안전보장이사회의 결의를 반영하여 불

법행위 유형을 확대하여 적용할 것을 요구하였다.

또한 해상테러 행위자를 보다 용이하게 추적하여 처벌할 수 있는 근거를 마련하기 위하여 선박 소유권과 관리의 정의 문제에 대해서는 승무원 임명 권한을 가진 자, 선박의 사용 및 운영 권한에 대한 결정권을 가진 자, 선박소유자를 대리하여 용선계약에 서명하는 자 등으로 의견을 모았다.

국제해사기구는 2005년 SUA 협약 및 의정서 개정안을 채택하여 해상 테러를 범죄행위로 추가하였고, 선박 등 해상운송수단을 이용한 새로운 양상의 해상 테러 행위를 처벌과 테러·WMD(Weapons of Mass Destruction) 운송 혐의선박에 대하여 기국의 동의를 조건으로 승선하여 검색가능 하도록 법적 제도를 신설하였다.

해상 테러 및 WMD 운송 범죄 관련자에 대한 범죄인 인도와 형사사법 공조체제를 수립하고 위반자에 대한 국제적 진압과 처벌을 강화하였다.

이와 같이 해상불법행위억제협약(SUA)은 2004년 7월 발효된 국제선박 및 항만시설 보안규칙(ISPS Code)과 해상인명안전협약(SOLAS 협약)을 보완하여, 해상 테러를 국제법상의 범죄로 규정하여 선박이 테러 수단으로 사용되는 것을 방지하고 선박 항행의 안전 확보를 목적으로 한다.[1] 2017년 IMO 해사안전위원회의 제98차 회의에서는 해상보안 강화를 위한 조치와 선박에 대한 해적 및 무장강도 범죄에 대하여 집중적으로 논의되었다.

GISIS(Global Integrated Shipping Information System)의 해상보안 모듈로 정보전송을 위한 지침서가 개발되고 있으며, 기니만(GoG: Gulf of Guinea)지역의 해적신고센터(IMB PRC)와 해양정보통합망(MDAT-GoG)에 선박에 대한 해적 및 무장강도 사건에 대한 보고를 독려하기 위해 결의서 초안(Reporting of Incidents

1)김태운, “한국 해운의 소말리아해적 재판의 분석과 국제법적 검토”, 「해사법연구」, 23, pp.67-100.

Piracy and Armed Robbery Against Ships in the Gulf of Guinea)도 승인되었다.

이에 따라 선장・선주・선박운항자・해운회사 등은 선박에 대한 해적 및 무장강도 행위에 의한 사고와 의심상황에 대해 이메일 또는 전화로 GoG 지역의 해적신고센터(IMB PRC) 및 해양정보통신망(MDAT-GoG)에 보고하여야 한다. 사고 보고가 활성화 될 경우에는 보고된 정보에 기반하여 대책을 마련하는 등의 조치를 취할 수 있어 GoG에서의 관련 사고 감소에 기여할 것으로 기대하고 있다.

따라서 본 연구에서는 선박 보안사고 실태 및 그 원인을 파악하여 선박 보안 관리의 특성을 고찰하고 선박 보안 관리 시스템의 취약성을 분석하고자 한다.

또한, 해상공급사슬보안(Maritime supply chain security)의 개념과 특징, 보안위험과 공급사슬의 취약성을 파악하고, 국제기구의 해상공급사슬보안제도와 주요국의 해상공급사슬보안 인증제도에 대한 현황 분석 및 시사점을 도출하여 해상공급사슬보안의 문제점 개선과 해상물류 전 구간에서 발생할 수 있는 보안 사고를 사전에 예방하는데 주안점을 두었다.

그리고 선행연구를 검토하여 해운기업의 해상공급사슬보안 요소 및 범위를 설정하고, 해운기업의 보안위험 예방 대책과 위험성을 낮출 수 있는 방안을 모색하고자 하였다.

이를 통해 각 종 해상 보안위험에 효과적으로 대처하기 위한 인적, 물적 보안시스템을 구축하여 해운기업의 보안 사고에 대한 효과적인 위험관리 전략을 제안하였다.

제2장 선박 보안사고 현황

제1절 선박 보안사고 실태

해상교통의 특성인 고립성, 고위험성, 국제성, 자연현상 의존성 등을 고려한 인명과 선박, 환경 안전 등에 대한 각종 협약도 발효되어 국제적인 협력 체계가 확립되고 있다. 특히, ISM(International Safety Management) code의 도입으로 해난 방지를 위한 안전관리체계와 안전문화가 정착되어 가고 있다.

그러나 9·11 테러 사건 이후로 해양안전(maritime safety) 대책과 함께 해양보안(maritime security)에 대한 대책이 요구되고 있다. 국제적 이슈가 되었던 해상테러 사건으로는 1985년 10월 이집트 연안에서 이탈리아 여객선 Achille Lauro호의 납치사건과 2002년 10월 예멘에서 발생한 미구축함 Close호 폭탄공격사건, 2002년 10월 예멘에서 일어난 프랑스 국적의 유조선 Limburg에 대한 탄이 실린 소형보트에 의한 자살테러 사건 등이 있다. 2004년 4월 이라크 움카사르 항에서 약 160km 떨어진 걸프해역의 원유 터미널과 저장탱크에 폭발물을 장치한 소형보트를 이용한 자살테러 사건이 발생하였다. 또한 2010년에는 싱가폴 부근 해역에서 이슬람 과격단체의 대형 유조선 공격 사건과 호르므즈해협(오만 영해)에서 알 카에다 소행으로 마샬군도 선적의 유조선 엠스타호 폭발 사건이 발생하였다.

선박 보안사고는 선박 자체를 무기로 이용하여 육상의 시설물을 공격하거나, 대량 테러 무기의 운송수단으로도 이용된다는 특징이 있다. 항만 및 선박, 해양시설의 취약한 보안 문제가 노출되면서 해상 테러 행위에 대한 대책 마련을 위한 국제적인 관심이 높아지고 있다. 기존의 해적행위 및 밀수나 밀항, 마약유통과 같은 단순히 경제적 이익을 목적으로 하는 해상 보안 위협에서 정치, 종교적인 관점에서

조직된 단체로부터의 테러와 대량 살생 무기유통 등 해상에서의 위험성은 더욱 높아지고 있다.

해상에서의 납치 및 해적사건은 지속적으로 발생하고 있으며, 이러한 해상 보안사고에 무기의 사용이 현저히 증가하고 더욱 조직적이고 광범위한 시도가 늘어나고 있다. 해적은 항만, 협수로, 연안지역 등 여러 지역에서 상선에 심각한 보안 위협을 가하고 있다. 최근에는 서아프리카 기니만 해역과 싱가포르-말라카 해협 및 동남아시아 해역에서 상선을 공격하는 해적이 늘고 있다. 우리나라의 선박 또한 여러 차례 공격을 받은 사례가 있다. 2011년 1월 아랍에미리트에서 출항하여 스리랑카로 항해 중이던 케미컬선 삼호주얼리호가 아라비아해 인근에서 소말리아 해적에게 피랍되었으며 우리 해군 청해부대의 구조작전으로 구출되었다.

소말리아 해역은 연합해군의 해적퇴치 활동 및 해상특수경비원의 승선 등을 통해 다각도에서 해적대응 노력을 하고 있어 해적활동은 크게 위축되었다. 2017년 3월 이후 소말리아 해적활동 재개에 따라 소말리아 해역에서의 해적피해가 우려되고 있다. 서아프리카 기니만(나이지리아) 인근 해역 해적활동이 2015년 다소 감소했었으나, 그 이후로 크게 증가하고 있다. 석방금을 노린 선원납치가 지속적으로 발생하고 있다.

동남아시아는 전통적으로 싱가포르-말라카 해협 등지에서 해적활동이 가장 많은 지역으로 평가되고 있다. 동남아 각국의 적극적 해적대응활동 및 아시아지역 해적퇴치협정(ReCAAP)을 통한 지역 협력의 결과로 해적사고는 감소하였다. 최근 Sulu-Celebes Sea 해역에서는 석방금을 노려 선원 납치가 급증하고 있는 실정이다. 필리핀 Abu Shyyaf Group이 선원납치사고의 대부분을 차지하고 있다. 이에 필리핀 정부는 동 조직에 대한 토벌작전을 실시하고 있다.

전 세계 해적 및 무장강도의 발생 추이, 주요 발생 지역과 특징은 다음과 같다.

<표 2-1> 전 세계 해적 및 무장강도의 발생 추이, 주요 발생 지역과 특징

연도	해적 및 무장강도 발생 건수	지역별 해적 및 무장강도 발생현황						해적 및 무장강도 공격유형				
		동남아	극동	인도	남미	아프리카	기타	침입 시도	총기 발사	침입	피랍	행방 불명
2008	293	54	11	23	14	189	2	47	46	151	49	0
2009	410	46	23	30	37	266	8	85	121	155	49	0
2010	445	70	44	28	40	259	4	89	107	196	53	0
2011	439	80	23	16	25	293	2	105	113	176	45	0
2012	297	104	7	19	17	150	0	67	28	174	28	0
2013	264	128	13	26	18	79	0	28	22	202	12	0
2014	245	141	8	34	5	55	2	28	13	183	21	0
2015	246	147	31	24	8	35	1	27	1	203	15	0
2016	191	68	16	17	27	62	1	22	12	150	7	0
2017	180	76	4	15	24	57	4	22	16	136	6	0
합계	3010	914	180	232	215	1445	24	520	479	1726	285	0

자료: 한국해양수산개발원.

UN 해양법 상에 해적(Pirate)은 민간선박 또는 민간항공기의 승무원이나 승객이 사적 목적으로 공해상의 다른 선박이나 항공기 또는 그 선박이나 항공기내의 사람이나 재산 또는 국가 관할권에 속하지 아니하는 곳에 있는 선박·항공기·사람이나 재산에 대하여 범하는 불법적 폭력행위, 억류 또는 약탈행위로 정의되어 있다. 또한 어느 선박 또는 항공기가 해적선 또는 해적항공기가 되는 활동을 하고 있다는 사실을 알고서도 자발적으로 그러한 활동에 참여하는 모든 행위, 규정된 행위를 교사하거나 고의적으로 방조하는 모든 행위를 포함한다.[2)]

그런데 최근 새로운 종류의 해적이 등장하여 항만시설과 선박 등의 테러가 증가할 것으로 예견되어, 조선해양 관계 기업과 조직이 긴장하고 있다. 선박의 안전을 위협하는 요소로 화재, 폭발, 해적이나 테러단체 등에 의한 납치였다. 그러나 최근에는 ICT(정보통신기술)와 융합되며 사이버 해적(Cyber Pirate)이 새로운 위협 요소로 부상하고 있다.

2) UN 해양방지법 제101조 해적행위의 정의

최근 들어 사이버 해적에 의한 공격 사례를 다수 접할 수 있다. 2010년 한국에서 남아메리카로 가는 시추선의 제어 시스템이 악성코드에 감염되었고, 원상 복구하는데 19일이 소요된 사건이 발생했다. 2011년 이란의 해운기업 Iranian Shipping Line의 서버에 사이버 해적이 침입하여 적재화물의 종류와 화물번호, 운송날짜 및 장소 등의 데이터를 손상시켜 잘못된 곳으로 화물이 운송되거나 분실되었다.

사이버 해적의 공격은 이뿐만이 아니었다. 2013년 벨기에의 항만 제어시스템에 사이버 해적이 침입해 마약의 일종인 코가인, 헤로인을 다른 화물로 밀반입/출하였다. 2016년에는 벨기에 마약 밀매업자가 해커를 고용해서 2011년부터 2013년까지 마약이 담긴 컨테이너 위치를 찾아내기 위해 앤트워프 항만제어 시스템을 해킹한 사례가 있다. 또한 글로벌 해운기업의 선적 화물 관리 시스템과 선하증권 관리 시스템에 사이버 해적이 침입하여 화물 정보와 선박 운항 일정을 파악하였고, 선박 납치 후 특정화물이 적재된 컨테이너만을 강탈한 사건이 발생했다.

2017년 6월 세계 최대 해운기업 머스크라인의 IT 시스템이 랜섬웨어(낫페트야) 공격으로 다운되어 4,000여대의 서버와 4만 5,000여대의 PC, 2,500여개의 앱 재설치 등으로 피해액만 약 3,000억원대에 이르렀으며, 선사 귀책사유에 의한 화물도착 지연으로 전세계적인 이슈가 되었다.

2018년 4월 나이지리아의 사이버 해적인 골드갈레온(Gold Galleon)이 한국 해운기업 Korean Shipping Firm을 포함하여 9개국 해운기업을 공격했다. 임직원의 이메일 아이디와 패스워드를 유출하여 고객 대금청구 주기와 선박 스케줄을 알아내어 90만 달러의 탈취를 시도한 사건이 밝혀졌다.

4차 산업혁명시대에 따라 앞으로는 더욱 치밀해진 사이버 공격이 해운기업을 위협할 것으로 예상된다. 이에 따라 세계 각국은 사이버보안 대책을 서둘러 수립하고 있다.

제2절 선박 보안사고 원인

테러리즘이라는 용어는 9·11 테러사건 이전과 이후로 나누어 볼 수 있다. 9·11 테러사건 이전의 정의에서 '테러리즘'이란 정치적 동기를 가진 계획적인 폭력으로 일반적으로 공중(公衆)에게 피해를 입히는 행위이며, 인명과 재산에 대한 위협과 강요, 위력 또는 폭력의 위법수단 행사를 통하여 정부 혹은 어떤 분야에 정치적·사회적 목적을 추구하려고 하는 행위로 볼 수 있다. 그렇지만 이때의 테러리즘은 사상의 차이나 좌익·우익여부, 유대주의에 의한 테러분자 또는 폭력에 의해 목적을 완수하려는 단체 등이 포함되는데 사상적 배경 또는 환경적 배경에 의한 테러리즘이 나타났다.

한편, 9·11 테러사건 이후 '테러리즘'에 대한 정의는 개념정의의 범위와 구성요건을 상세히 규정하고 있다. 9·11테러 이후 자금이나 모집 등의 활동에 대한 테러 대책이 최근 강화되고 있고, 테러를 지원하는 행위를 범죄화하는 등의 조치도 강구되고 있다.

테러리즘에 대한 공통된 인식이 충분하지 않은 환경으로 인해 상황에 대한 이해도와 접근법이 다를 수 있다. 그러나 테러리즘이 허용되지 않는 행위로 인지하고 있는 것이 일반적이다.

2003년 4월 부산의 국내 항만과 해역도 러시아 갱단에 의한 살인사건을 통해 테러의 위험에 노출될 수 있다는 것을 보여준다. 특히 해양을 이용하여 운항하는 상선은 선박 자체의 재산 가치와 탑승 인명 위협, 환경과 경제의 직·간접재해 등의 이유로 언론에 관심이 집중되어 테러 수단으로 이용될 가능성이 높다.

해상의 보안환경 및 선박의 보안 취약성은 다음과 같다.

첫째, 광대한 해양을 항로로 이용하므로 교통에 대한 통제와 제어가 어렵다.

둘째, 해안 근방에 있는 인구 밀집 지역 또는 대도시로의 접근이 용이하다.

셋째, 대량 화물 운송이 대부분으로 위험물의 검사가 어렵고, 육상 교통수단과의 연계로 인해 확산이 쉽다.

넷째, 대부분의 상선에는 특별한 자체 보안장비가 없다.

다섯째, 테러 관련자 등의 선박에 대한 접근이 용이하다.

여섯째, 선박의 규모에 비하여 테러 대응 인원이 적다.

마지막으로 육상 테러 억제세력의 지원이 어렵다.

9·11 테러 이후 항만의 인프라 시설은 보안시스템 구축에 초점을 맞춰 왔다. 사실상 항만은 전 세계 교역량의 90~94%를 처리하며, 대규모의 금융거래가 이루어지고 이해관계자와의 중요 데이터가 교환되는 곳이지만, 그간 보안은 하드웨어에만 집중되어 있었다.

현재 선박은 네트워크 모니터링 시스템 및 네트워크 보안 장비의 부재, 소프트웨어 업데이트 부족 등으로 인한 다양한 사이버 위험에 노출되어 있다.

첫째, 개방형 네트워크에 대한 보안 프로세스와 시스템의 부재이다. 지금까지의 선박은 사이버 환경에서 발생되는 보안 사고의 방지를 위해서 선내 일부 거주 공간과 업무용 PC에서만 선육 간 통신을 허용하도록 네트워크를 구분하여 운영하고 있다. 하지만 조선해양기자재가 정보화, 네트워크화 되면서 장비 간, 시스템 간의 데이터 수집과 공유 등이 요구되고 있다. 특히 e-Navigation 서비스를 이용하기 위한 선육 간 통신 등이 필요하다. 이처럼 개방된 네트워크 환경에서 더욱 증가되는 선박 IT 장비에 대한 관리 및 보안이 시급한 상황이다.

둘째, 선박에 설치된 장비 및 네트워크에 대한 상태 모니터링과 네트워크 장비 관리 시스템의 부재이다. 현재 선내 네트워크는 단순히 방화벽과 게이트웨이로 분류되고 있으며, 네트워크 장비에 대한 상태 모니터링 및 통합관리, 비인가 장치에

대한 관리 등이 제대로 이루어지지 않기 때문에 이동매체에 대한 멀웨어(Malware)[3] 감염 등 다양한 위험이 존재하고 있다.

셋째, 제한된 해상통신 환경으로 인한 선내의 운영체계와 각 장비의 기능 구현을 위한 프로그램 소프트웨어의 업데이트가 원활히 이루어지지 않고 있다. 육상에서는 온라인으로 OS, 응용프로그램에 대한 최신의 패치 파일이 업데이트 되지만, 선박에서는 Table 1과 같이 제한된 해상 통신 환경으로 인해 온라인의 이용이 불가하고, 선박이 육상에 정박하면 업데이트 파일을 이동매체(CD, USB 등)로 전달받아 해당 컴퓨터에 수동으로 설치하고 있다.

뿐만 아니라 선박에 설치된 컴퓨터는 사람의 접근이 어려운 곳이 대부분이고, 수많은 선내 컴퓨터가 안전 패치조차 설치하지 않은 상태에서 운영되고 있어 사이버 공격에 대한 대응이 매우 취약하다.

넷째, 개인통신에 대한 보안과 관리 기술의 부재이다. 현재 대부분의 선박에서는 함교(Bridge)와 일부 업무용 PC에서만 선육간 통신을 허용하지만, 일부 해운선사는 선원복지를 위해 wi-fi 인터넷 등의 개인 네트워크 환경을 제공하고 있으며, 선원복지 및 근무환경 개선에 대한 요구로 인해 개인 네트워크 환경에서의 선육간 통신 서비스가 확대되고 있다. 하지만 아직까지 선박은 육상 수준의 보안 인프라가 구축되어 있지 않다. 다음 <표 2-2>와 같이 통신 속도와 요금에 제한이 많기 때문에 개인통신 사용량에 대한 통제가 필요하다. 특히 사이버 보안사고 대부분은 인적과실에 의한 발생이 대부분이기 때문에 개인 통신 환경시, 사이버 보안에 대한 대책이 필요하다.

---

3) 멀웨어(Malware) : 소유자의 승낙 없이 컴퓨터 시스템에 침입하거나 시스템을 손상시키기 위해 설계된 소프트웨어

<표 2-2> Maritime Satellite Communication System

System	Band	Range	Bandwidth	Comment
Inmarsat C	L	A3	9.6kbps, packet oriented	GMDSS, short e-mails
Inmarsat fleet	L	A3	128-450 kbps	GMDSS, supports internet
Iridium	L	A4	134 kbps (open port)	Also coverage in arctic.
VSAT shared link	C, Ku, Ka	A1-A3	Any, typical 64-512 kbps, shared by several users.	Normally not deep sea.
VSAT dedicated link	C, Ku, Ka	A1-A3	Any, dependent on	
Other (Orb-comm, ect.)				

다섯째, 안티바이러스 기술의 부재로 인해 멀웨어(malware, malicious software)와 같은 악성 소프트웨어, 에드웨어(adware)[4]를 통한 바이러스 침투 등이 증가하고 있다. 육상에서는 안티바이러스 프로그램을 필수적으로 사용하고 있으나, 해상의 경우 거의 적용되지 않는다. 일부 최신 솔루션을 사용하는 대형 해운선사에서도 선내 장비 업그레이드 방법은 동일하게 항만 입항 시 안티바이러스의 최신버전을 이동매체를 이용하여 업데이트하고 있는 실정이므로 진화하는 사이버 위험에 대한 적극적인 대처가 필요하다.

4) 에드웨어(adware) : 광고를 보는 것을 전제로 하여 사용이 허용되는 프로그램

제3장 이론적 고찰

제1절 해상공급사슬보안 (maritime supply chain security)

1. 해상공급사슬보안의 개념

해상공급사슬보안에 대한 연구를 위해서는 먼저 관련 용어와 그 개념을 파악할 필요성이 있다. ISO 28000:2007에서 공급사슬(Supply chain)은 '원재료 조달에서 시작하여 운송모드를 거쳐 최종 이용자에게 제품 또는 서비스 인도까지 확대되는 자원 및 프로세스의 연결 세트'라고 정의하고 있다. 공급업체. 제조시설, 물류공급자, 내부 유통센터, 유통업체, 도매업체 및 최종 이용자에게 전달하는 기타 단체를 포함한다(ISO 28000:2007).[5]

보안(Security)은 '공급사슬에 대해 또는 공급사슬에 의하여 피해 또는 손상을 주기 위하여 계획된 고의적이고 허가되지 않은 행동에 대한 대처'라고 정의하고 있다(ISO 28000:2007).[6] 보안경영(Security management)은 '조직이 조직의 리스크, 잠재위협 및 이에 따른 영향을 최적으로 관리하는 체계적이고 조직화된 활동 및 실행'이라고 규정하고 있다(ISO 28000:2007).[7]

---

5) ISO 28000:2007, 3.9, supply chain : linked set of resources and processes that begins with the souring of raw material and extends through the delivery of products or services to the end user across the modes of transport(Note : The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesales and other entities that lead to the end user).

6) ISO 28000:2007, 3.2, security : resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain.

7) ISO 28000:2007, 3.3, security management : systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts therefrom.

공급사슬보안경영(Supply chain security management)에 대하여 '공급사슬 자산(제품, 시설, 장비, 정보 및 사람)을 도난, 손상 또는 테러로부터 보호하고, 허가받지 않은 금지품목, 사람 또는 대량 살상무기가 공급사슬로 유입되는 것을 방지하기 위한 방침, 절차, 기술의 적용'으로 정의하고 있다(David Closs, 2008).

즉, 해상공급사슬보안(Maritime supply chain security)은 '해상공급사슬에 대해 또는 해상공급사슬에 의하여 피해 또는 손상이 발생하도록 계획된 고의적이고 허가되지 않은 행동에 대한 대처'로 정의할 수 있다.

또한 해상공급사슬보안경영(Maritime supply chain security management)은 '해상공급사슬에 허가받지 않은 금지품목, 사람 또는 대량 살상무기가 공급사슬로 유입되는 것을 방지하기 위한 방침, 절차, 기술을 적용하여 해상공급사슬 자산(화물, 항만, 선박, 해운기업 및 화물과 선박의 정보 및 승무원)을 도난, 손상 또는 테러로부터 보호하고, 리스크와 잠재위협 및 이에 따른 영향을 최적으로 관리하는 체계적이고 조직화된 활동 및 실행'으로 정의할 수 있다.

2. 해상공급사슬보안의 특징

해상공급사슬보안은 공급사슬 자체에 침투하는 위협을 예방하거나 대응하는 관점에 집중되어 왔다. 화물, 항만, 선박 및 서비스 등의 흐름을 안전하게 관리하여 원활한 교역을 유지하는 것이 해상공급사슬보안의 궁극적인 목표로 인식되어온 것이다.

반면, 9·11테러 이후부터 해상공급사슬 또는 교역 자체가 위협을 야기하거나 해상공급사슬을 매개로 한 위협에 대한 인식이 확산되어 왔다. 테러리스트가 선박 자체를 테러의 도구로 삼는 것과 같이 해상공급사슬 자체를 무기로 이용할 수 있다는 점에서 문제 인식이 증폭된 것이다. 또한 마약과 같이 허가받지 않은 금지품목 또는 대량 살상무기 등 불법 화물의 운송은 해상공급사슬을 매개로 한 위협으

로 볼 수 있다. 컨테이너 선박의 대형화 및 고속화 추세로 불법 화물의 은닉 수단과 운송 매개체가 증가됨에 따라 해상공급사슬보안은 더욱 위협받고 있다. 그리고 최근 증가하고 있는 사이버 해적의 공격은 화물 정보와 선박 운항 스케줄 등을 이용한 정보 교란과 차단으로 그 심각성은 가중되고 있다. 이와 같은 유형의 위협으로 인하여 인명 손실과 핵심 사회 간접자본 등 심각한 물적 손실이 발생할 수 있다. 따라서 해적에 의한 선박 납치와 화물 절도, 강탈 등과 같이 기존의 공급사슬 자체에 대한 위협에 비하여 매우 심각한 결과를 초래할 수 있어 이에 대한 체계적이고 조직적인 대책 수립이 중요하다.

그리고 이러한 유형의 위협은 경제적 측면과 안보적 측면에서 문제를 야기한다. 공급사슬보안의 확보는 재화와 용역의 적법한 거래를 보장하며, 공급사슬이 테러의 도구로 사용되는 것을 방지하는 차원에서 그 중요성이 인식되고 있다.

앞서 해상공급사슬보안(Maritime supply chain security)은 '해상공급사슬에 대해 또는 해상공급사슬에 의하여 피해 또는 손상이 발생하도록 계획된 고의적이고 허가되지 않은 행동에 대한 대처'로, 해상공급사슬보안경영(Maritime supply chain security management)은 '해상공급사슬에 허가받지 않은 금지품목, 사람 또는 대량 살상무기가 공급사슬로 유입되는 것을 방지하기 위한 방침, 절차, 기술을 적용하여 해상공급사슬 자산(화물, 항만, 선박, 해운기업 및 화물과 선박의 정보 및 승무원)을 도난, 손상 또는 테러로부터 보호하고, 리스크와 잠재위협 및 이에 따른 영향을 최적으로 관리하는 체계적이고 조직화된 활동 및 실행'으로 정의하였다.

이에 따라 단편적이고 부분적인 활동에서 벗어나 조직이 수행하는 프로세스의 모든 부분에 적용되어야 한다. 또한 조직 구성원 모두에게 적용할 수 있는 보안경영활동을 분석하고 구체화해야 한다.

3. 보안위험과 공급사슬의 취약성

1) 보안위험

영국의 Cranfield 대학의 연구보고서[8]에서는 공급사슬 취약성(vulnerability)을 “공급사슬의 외부적인 위험뿐만 아니라 내부적인 위험으로부터 발생하는 심각한 혼란에 대한 노출”로 정의하고 있다.

물품의 조달, 생산, 판매 및 인도에 이르는 공급사슬상의 모든 활동은 서로 연계되어 있으므로, 글로벌 공급사슬의 운영과정에서 발생하는 변동에 따라 공급사슬 전반에 미치는 효과가 크고 공급사슬 구조를 불안정하게 만들 수 있다.

공급사슬의 취약성을 높이는 공급사슬위험요인[9]으로는 테러 및 보안위협 외에도 허리케인이나 홍수, 지진과 같은 자연재해에서부터 공장가동 중단, 자재부족과 같은 운영상의 혹은 일상적 위험, SARS와 같은 전염병, 사보타주와 같이 인간에 의해 행해지는 재난, 그리고 세관검사로 인한 통관지연, 운송지연 등에 이르기까지 다양하다.[10] 자연재해나 동맹파업 혹은 테러리스트들의 공격과 같은 외부적인 요인들뿐만 아니라 기업의 경영전략의 또한 공급사슬구조에 영향을 미칠 수 있다.[11]

최근 기업들은 JIT 생산방식 및 린(lean) 관행을 채택하고 생산 및 물류시설을 집중하는 한편, 아웃소싱은 늘리되 공급선을 단순화하는 등 공급 사슬상 재고 및 낭비

---

8) Cranfield School of Management (2002), Supply Chain Vulnerability, report on behalf of DTLR, DTI and Home Office.

9) 공급사슬 위험은 최초 공급자로부터 최종 소비자에 이르기까지 계획된 물자의 흐름을 방해하거나 중단시키는 우연한 사건으로 정의할 수 있다(Donald Waters, Supply Chain Risk Management, KOGAN PAGE, 2007, p.7).

10) Ravi Sarathy, “Security and the Global Supply Chain”, *Transportation Journal* , Fall 45, 4, 2006, p.30.

11) John F. Frittel, “Port and Maritime Security: Background and Issues”, *Military Technology*, Nov. 2006, pp.88-94.

요소을 제거하거나 줄임으로써 공급사슬의 효율성을 높이는데 주력해 왔다. 이러한 전략은 시장상황이 안정적인 경우 공급사슬의 효율성을 증가시키지만 시장상황이 불안정한 경우에는 공급사슬의 취약성을 높이는 원인이 되고 있다.[12] 공급사슬상 파트너의 수와 규모, 경험, 그리고 능력은 모두 공급사슬 보안에 영향을 미친다. 공급자의 수가 적을수록 보안사고 발생시 대안적인 공급선을 확보하기 어렵기 때문에 공급중단으로 인한 공급사슬 혼란이 발생할 가능성이 커지게 되며 마찬가지로, 공급사슬 파트너의 규모가 작을수록 공급사슬보안에 대한 투자가 제한을 받을 수 밖에 없기 때문에 공급사슬 전반에 걸쳐 동일한 수준의 보안을 확보하기 어렵다.[13]

Hendrick and Singhi(2005)는 지나치게 효율성을 강조하는 공급사슬 구조는 공급사슬 혼란에 대한 취약성을 높일 수 있다고 하였다. 마찬가지로 외부조달에 대한 의존도가 높은 공급사슬의 경우 위험에 취약하다. 이러한 구조를 가진 공급사슬하에서 보안관련 위험 발생가능성이 높게 나타난다.

2) 국제물류보안제도의 강화

공급사슬상의 보안이 확보되지 않으면 개별기업 및 경제전반에 영향을 미칠 수 있다는 점에서 미국을 비롯하여 세계 각국 및 다국적 정부기구에서는 국제 물류보안제도를 강화하기 위한 법규 및 정책들을 개발해왔다. 물류보안제도는 ISPS Code와 같이 IMO나 WCO와 같은 국제기구를 중심으로 도입된 강행적 규제와 CSI, C-TPAT와 같이 참여 당사자에게 경쟁적인 이점을 제공한다. 이를 통해 물류보안을 강화하는 한편, 물자의 이동을 촉진하기 위한 자율규제 프로그램들을 강화한다. 이들 보안프로그램들의 주된 목적은 국제물류시스템상의 테러위협을 줄이

12) Kevin B. Hendrick and R. Vinod Singhal, “An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm”, *Production and Operations management*, 2005, 14(1), pp.35-52.

13) Ravi Sarathy op. cit., pp.41-42.

고 물류보안을 강화하기 위한 것이다. 따라서 기업 입장에서 이들 프로그램을 준수하고 이행하기 위해서는 많은 시간과 비용이 소요[14]될 뿐만 아니라, 이러한 제도 자체가 공급사슬의 효율성 및 효과성에 심각한 부작용을 초래할 수 있음을 우려하고 있다.

3) 물류보안비용

9.11 사태는 1천 9백억 달러에 달하는 피보험 재산과 약 900억 달러에 달하는 경제적 손실을 초래하였다.[15] 양정호(2008)의 연구에 의하면, 테러리즘의 직접적인 결과로 발생하는 비용은 인명의 손실, 재산의 파괴, 단기적 경기침체 등을 들고 있다. 이들 비용은 지속적인 테러위협으로 인한 불확실성이 증가함에 따라 예방을 위한 자원비용까지 더욱 증가하고 있다.

공급사슬보안체계를 구축하기 위해 불가피하게 발생하는 비용들이 있다. 정부에서 일정수준의 화물보안을 강행적으로 요구할 수 있고, 미국 국토보안국(DHS: Department of Homeland Security)과 같이 보안책임을 담당하는 정부기관에서 보안비용 명목으로 새로운 요금을 징수할 수도 있다. CBP(Bureau of Customs and Border Protection)와 같은 정부기관의 규제는 컨테이너 봉인의 채택을 증대시킬 수 있고 CSI나 C-TPAT와 같은 보안프로그램 참여의 유인을 제공할 수 있다.[16]

홍콩항에서 전수검사(universal screening)를 제안하거나, 컨테이너가 현물심사대상으로 선정되는 경우, 컨테이너의 양륙 및 검사에 소요되는 비용을 수반하게 된다. 각국 정부의 물류보안 강화에 따른 검사비율이 증가하여 항만혼잡이나 통관지연이 발생한다. 이로 인해 공항 또는 항만에서 내륙으로의 연계운송이 원활히 작

14) Russel and Saldanha(2003)는 보안관련 공급사슬 비용을 6천 5백억 달러로 추산.

15) William J. Stevenson, *Operations management*. McGraw-hill, 2005.

16) Ravi Sarathy op. cit., p.42.

동하지 않아 기업의 생산계획이나 배송계획에 차질을 발생할 수 있다. 이는 결국 기업의 재고수준 및 처리비용이 증가하여 기업의 운전자금 및 현금흐름에도 악영향을 미칠 수 있다.[17] 뿐만 아니라 검사과정에서 컨테이너 화물의 손상이 발생하는 경우 그 비용은 고스란히 운송인과 수입업자가 떠안게 된다. 또한 보안상의 문제가 발생한 컨테이너에 대해서는 벌금이 부과되며, 일정한 규제조치를 받게 된다. 이러한 비용이나 책임에 대한 분쟁이 발생할 소지도 있다. 공급사슬보안과 관련된 비용들은 운임이나 제품가격에 포함되어 최종 고객들에게 전가될 가능성이 높다.

Lee and Whang(2005)[18]은 공급사슬 혼란에 따른 비용 증가, 인도지연, 제품과 서비스의 원활한 흐름 방해, 리드타임 증가, 수량, 품질, 정시배송에 대한 불확실성 증대 등을 지적했다. 이에 따른 고객서비스 수준 하락에 따른 기업 매출 하락, 보안 및 기타위험의 증대로 인한 보험료 상승 등과 같은 간접적으로 영향을 미칠 수 있다.

이와 같이 해상 안전 보안체제가 국제적으로 강화되고 있는 것은 상존하고 있는 테러 위협에 따른 불가피한 조치로 파악된다. 최재선 등(2006)은 공급사슬에서의 테러 공격 유형에 대하여 다음과 같이 설명하고 있다.[19]

테러는 정치·종교·이념과 관련된 목적을 달성하기 위해 어떤 정부에 정치적 압력을 가하는 행동으로 정의할 수 있다. 운송시스템을 이용한 테러 공격 형태는 크게 두 가지로 나누어질 수 있는데, 첫째, 대량의 인명피해 또는 운송 인프라 공격을 통해 대중 매체를 이용하여 공포심을 유발하거나 국민의식에 영향을 끼치는 방법이다. 둘째, 물류 인프라를 파괴함으로써 장기적인 운행 중단을 통한 경제적

17) John F. Frittel op. cit., pp.88-94.

18) Hau L. Lee and S. Whang, "Higher Supply Chain Security with lower cost: Lessons from total quality management", International J ournal of Production Management, Vol. 96, 2005, pp.289-300.

19) 최재선 외, "국가물류보안 체제 확립방안 연구(I)", 한국해양수산개발원, 2006, pp.19-20.

손상을 가하는 방법이다. 이러한 테러는 가용한 정보의 제약으로 인해 예측이 거의 불가능하기 때문에 미연의 방지가 어려워 피해가 더욱 크다.

운송시스템을 이용한 테러 공격은 전 공급사슬에서 특정부분의 취약성과 밀접한 관계가 있는데, 이로 인해 인명 피해와 경제적 피해를 발생하는 것이다. 공급사슬에서 테러의 대상은 크게 세 가지로 나눌 수 있다. 첫째 화물 운송에 사용되는 모든 시설 즉 물류 인프라와 둘째 물류시설 운영 측면에서 화물의 흐름을 통제하는 모든 활동, 셋째 화물 그 자체가 공급사슬망의 흐름에 따라 움직이는 실체이다.

아래 <표 3-1>는 선박의 잠재적 테러 공격 대상을 요약한 내용이다.

<표 3-1> 선박의 잠재적 테러 공격 대상

구 분		테러 공격 대상
물류 인프라	운송로	해상로
	환적 장소	항만 터미널
시설 운영	통제 시스템	해상운송 관리 시스템
	통신 시스템	통신망
	종업원	선원, 하역 인력 보수 인력, 정보처리 인력
	운송수단	선박, 바지
운송 화물		비위험화물, 폭발화물 유독물, 가연화물

자료 : 김영균, “항만터미널의 유형과 공급사슬보안경영 활동이 경영성과에 미친는 영향에 관한 연구”, 한국해양대학교 박사학위논문, 2011.

운송시스템상의 보안 위험을 두 가지로 구분할 수 있다. 첫째, 운송 인프라의 보안위험은 공급망의 물류 흐름을 방해할 목적으로 테러범이 인프라를 손상시키거나 파괴하는 것이다. 둘째, 공급망 보안 위험은 운송수단인 차량, 선박, 항공기 등에 폭발물을 은폐하여 운송하거나 위험화물을 이용하여 목표하는 시설을 파괴하거나

사상자를 발생시키는 위험을 말한다.

특히, 해상운송에 있어서의 물류 사슬 테러는 경제적 활동뿐 아니라 세계 무역에 상당한 영향을 미치는 것으로 인식되고 있는데, 미국의 경우 지속적인 테러위협으로 인해 투자가 GDP의 2% 가량 감소한 것으로 분석되고 있다(Saxton, 2002). 또한 향후 발생할 위험이 있는 테러에 대한 영향력도 선진국뿐 아니라 개발도상국에서까지 작용하고 있다. 예로서 APEC지역의 일부 국가는 해상운송 부문에서의 테러에 대한 취약성이 높으며, 지속적인 해적행위의 발생으로 인해 외국인 직접투자가 감소한 것으로 나타났다.

(1) 인프라 보안 위험

테러 공격 대상 중 물류인프라의 경우, 철도·도로의 터널 및 다리, 복합운송/항만/물류 터미널, 철도 정차 야드, 교통 통제 시스템, 철도 시스템, 전원 공급기지, 수로 등이 될 수 있다. 물류 인프라 대상 테러는 운송 연계 부분을 마비시킴으로써 물류 흐름에 영향을 미치고, 결국에는 우회, 지체, 운송 형태의 전환 등을 발생시킨다. 김영균(2011)의 연구에 의하면, 운송비용과 파괴된 시설의 재건 비용 등으로 경제적 손실이 추정되며, 파괴된 시설에서 처리하는 화물의 물동량과 종류, 대체 운송수단 유무, 복구 소요시간 등에 따라 추가 운송비용이 달라진다.

(2) 공급사슬 보안 위험

테러범이 공급사슬을 악용하는 테러를 의미하는데, 운송 시스템은 테러의 대상이 아닌 수단으로 이용된다. 공급사슬을 악용한 피해사례는 크게 두 가지로 분류할 수 있는데 먼저, 트럭, 선박, 항공기 등의 운송수단을 이용한 테러이다. 공급사슬을 통해서 전 세계로 다양한 화물이 운송되고, 이 화물은 원료를 포함하여 완제품, 반제품 등의 형태로 소비자에게 배송되기까지 다양한 시설과 장소를 거치며 인구가 밀접한 지역을 통과하게 된다.

이 때 운송시스템뿐만 아니라 화물은 폭발물이나 독극물을 은폐하는 장소로 이용되고 테러범들이 원하는 장소로 이동시켜 피해를 가할 수 있다. Abt Association Inc.는 이런 종류의 피해 분석에 대한 연구를 진행하였는데, 이 연구 결과에 따르면 미국의 항만에 핵폭탄 및 생화학 무기를 이용한 공격이 가해지게 되면, 인적·경제적 피해는 <표 3-2>와 같이 추정되었다.

<표 3-2> 보안 위험 피해 예측

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

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

두 번째 사례는 위험화물, 즉 가연성 가스나 독극물 탱크를 이용한 테러이다. 이 때 테러범은 특별히 폭발물이나 생화학 무기를 은폐한다. 이로써 이동시킬 필요 없이 위험화물 자체가 인구 밀집 지역, 터널 및 주요 건물로 이동할 때에 공격을 가하므로 대량의 사상자와 경제적 피해를 발생시킨다.

예를 들어, LPG 40톤이 폭발될 경우 반경 150m 내의 건물이 파괴되고 사상자가 발생되며, 반경 300m 내에서도 사상자가 발생, 반경 500m 내에는 치명적인 부상자가 발생하는 것으로 분석되었다. 또한 가솔린 1,000kg이 방출되었을 경우에는 바람의 영향 없이 약 200명의 사상자가 발생된다. 바람이 있을 경우 약 1,000여명의 사상자가 발생하는 것으로 분석되었다. 1984년 12월 인도 보팔(Bhopal)시에 소재한 화학공장에서 메틸이소시안염이 탱크에서 누출되어 사상자가 거의 4,000명에 육박하였다. 1978년 7월 스페인 산카로스에서 발생한 무색의 가연성 가스인 프로필렌 폭발

사건 때에는 217명의 사상자가 발생하였다.

특히 항만이나 선박 등 물류시설은 테러리스트의 공격 대상이 될 가능성이 매우 높다. 항만을 대상으로 공격할 경우, 그 배후에 도심이 위치하고 있으므로 테러의 효과가 크고 일시에 수출입 물류를 마비시킬 수 있어 그 효과를 극대화시키기에 적합하기 때문이다.

이와 같이 해상 안전 보안제도 정비와 각종 물류 네트워크의 안전성 확보가 자국의 영토와 인명을 보호할 수 있는 원동력이자 국가 경쟁력을 확보하기 위한 핵심요소가 된다.

제2절 국제기구의 해상공급사슬보안제도

1. 국제표준화기구의 ISO 28000

국제표준화기구(International Organization for Standardization: ISO)에서 2007년 물류보안경영시스템을 ISO 28000 규격을 제정하였다. 물류보안인증제도 ISO 28000은 화물에 관한 정보와 화물을 제조 또는 운송 처리하는 사업자에 대한 규정 준수 여부를 미리 제공한다. 그리고 화물의 무결함을 보장받아 국제적으로 물류보안에 관한 인증 제도이다.

첫째, ISO 28000은 공급사슬을 관리하는 조직과 공급사슬에 포함된 제조, 서비스, 보관 및 운송 관련 조직에서 적용할 수 있도록 개발된 경영시스템으로서 공급사슬의 보안에 대한 리스크와 위협에 대한 관리를 하도록 요구한다.

둘째, ISO 28000은 화물의 흐름에 대한 효과적인 모니터링을 포함하여 밀수를 방지하고 해적의 위협이나 테러리스트의 공격에 대응하도록 할 뿐만 아니라 안전

한 국제적인 공급사슬시스템을 만들도록 설계되었다.

셋째, 조직이 공급사슬의 보안을 보장하는 데 필요한 핵심적인 측면을 포함하여 보안경영시스템을 수립, 이행, 유지 및 개선하도록 하는 요구사항을 담고 있습니다. 이러한 핵심적인 측면은 재무회계, 제조, 정보보안, 그리고 상품의 포장, 보관 및 수송시설을 포함한다.

1) ISO/PAS 28007 해상보안경영시스템

해적문제가 전세계 해운업계에 상업적인 위협이 증가함에 따라, 위험지역으로 이동하는 선박에 무장보안요원을 제공하는 민간해상보안업체(PMSC(Private Marintime Security Companies))가 증가하고 있다. ISO/PAS 28007은 이러한 법적, 안전성의 영향을 보장을 위하여 PMSC에 적절한 민간무장보안요원(PCASP(Privately Contracted Armed Security Personel))이 승선하는 것을 충족하기 위해 개발되었다.

SAMI(Security Association for the Maritime Industry)는 런던에 사무국을 둔 해상보안업계의 이익을 대변하는 대표적인 단체('11.4 설립)로서 34개국 147개 업체가 등록된 단체이며 전세계 해상보안업체의 75%가 SAMI에 등록되어 있다. SAMI에서는 IMO(국제해사기구)에서 개발된 PMSC의 적합성을 검증하는 프로그램이 있으며 ISO/PAS 28007인증은 이러한 SAMI의 심사를 면제 받을 수 있다.

ISO는 각국의 국가표준 관련 민간단체의 대표들로 구성된 비정부 국제기구이다. 그러나 ISO에서 제정한 규격은 일반적으로 국제협약이나 국가표준의 제정을 통해 제도화되기 때문에 다른 비정부 기구보다 영향을 크게 행사하고 있다고 할 수 있다. ISO는 2005년부터 ISO/PAS 280004) 형태로 공급사슬 보안경영시스템에 대한 국제표준을 제공하였다. 2007년 국제적으로 공인규격인 ISO 28000 시리즈를 공표하였다. ISO 28000 시리즈는 28000, 28001, 28003, 28004로 구성되어 있다. 특히

ISO 28000 시리즈는 공급사슬보안을 확보하기 위해 산업전반의 어느 조직에 적용될 수 있도록 제정된 보안경영시스템이며, 계획(plan)-실시(do)-점검(check)-조치(act)라는 PDCA 방법론에 기초하고 있다.[20] 즉, 조직이 지속적으로 보안환경을 평가하고 충분한 보안조치가 행해지고 있는지의 여부와 법제도 및 강제적 요구사항이 조직에 끼칠 영향을 지속적으로 모니터링하면서 문제점을 개선하는 것이다.

2) 보안기준 주요 내용[21]

ISO 28000의 보안기준은 일반요구사항, 보안경영방침, 보안리스크 평가 및 기획, 실행 및 운영, 점검 및 시정조치, 경영검토 및 지속적 개선의 6가지 영역으로 구성되어 있다.

<표 3-3> ISO 28000 시리즈

구 분	내용
ISO 28000	공급사슬 보안경영시스템(Specification for security management system for the supply chain)
ISO 28001	공급사슬보안, 평가 및 계획의 실행을 위한 모범 관행(Best Practices for implementing supply chain security, assessments and plans)
ISO 28003	공급사슬 보안경영시스템 심사 및 인증을 제공하는 기관에 대한 요구사항(Requirements for bodies providing audit and certification of supply chain security management systems)
ISO 28004	ISO 28000 실행 지침(Guidelines for the implementation of ISO 28000)

자료: ISP, Specification for Security Management Systems for the Supply Chain, 2007.

첫째, 일반요구사항으로 조직이 보안위험을 식별하고, 그 영향을 통제한다. 그리고 보안 위험을 최소화하는 보안관리시스템을 구축하고 실행·유지·개선하는 의무를 명시하고 있다.

---

20) 한국해양수산개발원, “해운과 경영”, 제24호, 2011. 6.

21) 고현정, “국제물류보안 인증제도 동향 및 시사점에 관한 연구”, 2011 내용 요약 및 재정리.

둘째, 보안경영방침으로 조직의 최고경영자가 조직의 보안관리 방침을 수립, 승인하고 문서화하여 관리해야 한다. 성공적인 ISO 28000 도입은 최고 경영자의 의지가 무엇보다 중요함을 강조하고 있다.

셋째, 보안리스크 평가 및 기획은 조직이 보안위협뿐만 아니라 보안경영 관련 리스크를 식별 및 평가하는데 있어서, 조직 내부적으로 문서화된 보안경영방침, 보안경영목표, 보안경영 세부목표를 수립하고 보안경영 프로그램을 통해 이를 실행해야 하는 내용이다.

넷째, 실행 및 운영은 조직이 보안경영의 방침, 목표, 세부목표, 그리고 프로그램에 대한 구성원의 역할, 책임, 권한을 명확히 하고, 특히 최고 경영자의 보안경영 시스템에 대한 이행 의지 중요성에 주안점을 두고 있다. 또한 보안경영에 필요한 장비, 도구 등의 설계, 설치, 운영, 개조 및 변경을 위한 인력교육 뿐만 아니라 훈련과 비상사태 발생 시 이에 대한 대응 및 복구에 관한 절차 수립도 포함한다. 이를 위해 종업원간 정보공유 및 의사소통 체계 마련도 중요하다.

다섯째, 점검 및 시정조치는 조직이 보안경영시스템의 성과를 모니터링하고 측정할 수 있는 절차를 마련하여 주기적으로 검토하고 부적합 또는 시정사항이 있을 경우 즉시 반영해야 한다는 내용이다. 이 절차들을 문서화하여 운영하고 그 성과는 지속적으로 관리되어야 하며, 보안경영 감사 프로그램을 활용하여 위협 및 리스크의 평가결과의 공정성이 확보되도록 해야 한다.

여섯째, 경영검토 및 지속적 개선은 보안경영시스템이 지속적으로 적절성, 충족성, 효과성 등이 보장되도록 계획된 주기로 최고경영자가 보안경영시스템을 검토해야 한다는 내용이다. 경영검토 대상은 리스크평가, 보안방침, 보안목표, 위협 및 리스크 등의 보안경영시스템의 전반적인 사항이며, 시스템의 변경 필요성도 또한 포함된다. 경영검토 이후 지속적 개선에 대한 의지 및 일관성이 보장되도록 보안

경영시스템의 변경과 관련된 의사결정 및 조치사항도 관리되어야 한다.

2. 국제관세기구의 WCO Framework[22)]

1) 개요

세계세관기구(WCO)는 2005년 6월 166개국 회원국 대표가 참석한 벨기에 브뤼셀 회의에서 물류보안과 무역 간소화에 관한 국제기준을 채택하였다(World Customs Organization, 2007). WCO Framework의 제정 목적은 크게 6가지로 요약될 수 있다. 즉, 국제수준의 공급사슬 보안확보 및 국제무역을 촉진하는 표준제공, 운송수단에 대한 통합공급사슬관리, 세관의 역할·기능·역량 강화, 고위험화물 적발능력 제고 및 각국 세관들과의 공조체제 강화, 세관과 민간기업 간 협력체제 강화, 보안확보를 통한 막힘없는 화물의 이동촉진이다. SAFE Framework의 구조는 6개의 장으로 구성되며, 세부적으로 서문, 혜택, 세관간 협정(Customs-to-Customs Network Arrangements), 세관-민간기업 협력(Customs-to-Business Partnerships), AEO 조건 및 자격요건, 결의안이다. 특히 세관간 협정과 세관-민간기업 협력이라는 두 가지 기능을 기초로 보안기준들이 국내외적으로 상호연계 되도록 하였다.

AEO 관련 세부적인 항목은 세관·AEO를 위한 조건 및 규정, AEO에 부여되는 혜택, 검증 및 공인, 화물처리 절차, 상호인증으로 요약된다. 특히 AEO 프로그램은 기업의 자율적인 참여를 바탕으로 하기 때문에 세관과 기업과의 협력체계 구축이 중요하다. 이를 위해 기업에 주어지는 혜택항목을 구체적으로 명시하고 있는데, 이는 민간기업이 보안강화를 위해 투자한 비용에 대한 보상기능과 기업의 적극적 참여를 유도하기 위함이다. AEO에게 제공하는 혜택들은 신속한 화물반출, 운송시간 절감, 창고비용 절감, 세관 정보의 접근 제공, 무역거래 위기상황 기간의 특별

22) 고현정, “국제물류보안 인증제도 동향 및 시사점에 관한 연구”, 2011 요약 재정리.

혜택, 신규 화물절차 프로그램 참여 우선권 부여 등이다. AEO의 범위는 화물의 국제이동에 관련된 당사자, 즉 제조업자, 수입업자, 수출업자, 중개인, 운송업자, 복합운송업자, 중재인, 항만, 공항, 터미널 운영사, 창고, 유통업자 등을 의미한다. 또한 세관은 AEO 검증 및 인증 절차를 마련해야 하는데 이는 각국의 실정에 맞게 제정하도록 하고 있다.

<표 3-4> WCO Framework 구조

목차	내용
서문	소개, 목적과 원칙, 4가지 핵심요소, Framework 구축, 능력배양, 이행조치
혜택	국가/정부, 세관, 민간
세관과 세관협정(Pillar 1)	세관당국 대 세관당국 간 표준, 표준이행을 위한 기술적 세부사항, 컨테이너화물의 안전을 위한 봉인관리
세관과 세관협정(Pillar 2)	세관당국 대 민간 간 표준, 표준이행을 위한 기술적 세부사항
AEO 조건, 자격조건 및 혜택	정의, 세관과 AEO를 위한 규정과 자격요건, AEO의 혜택 인증 및 승인절차, 관련 업계를 위한 절차개관, 상호인증

자료: WCO, WCO SAFE : Framework of Standards to Secure and Facilitate Global Trade(2007).

2) 보안기준 주요 내용

세관과 AEO를 위한 조건 및 규정은 13가지 항목으로 구성되어 있는데, 이 가운데 5가지는 AEO에게 적용되는 항목이며, 나머지 8가지는 세관과 AEO에게 공동으로 적용되는 항목이다. AEO에게 적용되는 항목은 세관요건 준수, 상거래관리 시스템 적합성, 재정능력, 무역파트너 보안, 측정·분석·개선이며, 세관과 AEO에게 공동으로 적용되는 항목은 상담·협력·의사소통, 교육·훈련·인지, 정보의 교환·접근·비밀보장, 화물보안, 건물보안, 운송보안, 인적보안, 위기관리와 사고복구이다.

AEO에게 적용되는 항목의 내용은 다음과 같다.

첫째, 세관요건 준수는 기업이 법제도를 위반한 사항과 관련하여 AEO의 자격에 대한 검토사항이다.

둘째, 상거래관리 시스템 적합성은 세관이 요구하는 기준에 따라 AEO가 수출입 관련 신뢰성 있는 자료 관리 시스템을 구축하고 있는지의 여부를 검토하는 항목이다.

셋째, 재정능력은 AEO가 공급사슬보안의 유지 및 향상 의무를 이행하기 위한 충분한 재정능력이 있는지의 여부를 판단하는 항목이다.

넷째, 무역파트너 보안은 공급사슬보안을 강화할 수 있는 신뢰성 있는 기업과 상거래관계를 형성하고 있는지의 여부를 검토하는 부분이다.

다섯째, 측정·분석·개선 부분은 기업이 보안평가를 수행하고, 보안관리시스템의 무결성 및 적합성을 보장하며 개선활동을 지속적으로 이행하고 있는지를 검토하는 내용이다.

AEO와 세관에게 공동으로 적용되는 항목은 다음과 같다.

첫째, 상담·협력·의사소통은 세관, AEO, 그리고 관련기관이 공급사슬보안 활성화 관련 사항들에 대해 상호이해를 돕기 위해 협의해야 하는 부분이다.

둘째, 교육·훈련·인지는 보안정책의 위반인지 및 위반할 경우 사후 조치 등에 대한 교육과 훈련절차를 마련해야 한다.

셋째, 정보의 교환·접근·비밀보장은 정보보안을 위해 정보의 오용이나 불법 변경을 방지하기 위한 수단을 개발하고 개선해야 한다는 내용이다.

넷째, 화물보안은 보관, 운송, 봉인 등의 물류활동에 따른 화물에 대한 보안확보를 위한 방안을 수립하고 강화책을 확보해야 하는 내용이다.

다섯째, 운송보안은 트럭, 운전자 등의 각종 운송수단과 관련된 보안확보가 효과적으로 관리되도록 협력해야하는 내용이다.

여섯째, 건물보안은 건물의 내·외부를 모니터하고 통제하는 규정을 개발해야 한다는 내용이다.

일곱째, 인적보안은 법적 근거에 따라 종업원의 신원을 조회하고 각종시설, 운송수단, 보관장소 등에 대한 비인가자의 접근을 방지해야 하는 내용이다.

여덟째, 위기관리와 사고복구는 재난이나 테러 위험을 최소화하기 위해 위기관리와 복구절차를 마련하여 특이한 상황에 대비해야 하는 내용이다.

3. 국제해사기구의 ISPS Code

2004년 7월 국제사회는 이와 같은 보안위험을 체계적이고 효율적으로 관리하여 해상에서 테러를 예방하고 퇴치하기 위하여 ISPS(International Ship and Port facility Security) code를 제정하였다. 심각해져가는 테러 위험시대에 선주와 항만당국은 물론 관련 종사자들도 선박테러에 대한 대비책 마련이 필요하다.

1) 개요

국제해사기구(International Maritime Organization : IMO)는 9.11 테러사건 이후 국제무역에 있어서 해상부문의 중요성을 인식하여 2002년 12월 12일 IMO 외교회의를 개최하여 해상인명안전협약(SOLAS)을 개정하여 선박 및 항만시석에 대한 보안강화 조치를 마련하였다. 본 개정에서는 SOLAS 제11-2장을 신설하여 해상보안 강화를 위한 특별조치를 규정하였으며, 이를 근거로 「국제선박 및 항만시설 보안규칙(International Ship and Port Facility Security Code, 이하 ISPS Code)」

을 채택하였으며, 2004년 7월 1일 국제적으로 발효되었다.

ISPS 규칙은 국제항해에 종사하는 각 선박과 관련 항만시설에 적용되며 보안을 위하여 체약당사국과 선사 및 선박이 준수해야 할 사항을 규정하고 있다. 그 구체적인 내용은 선박과 관련하여 자체보안계획을 수립하고, 자국정부의 보안심사를 받은 후 국제선박보안증서(유효기간 5년)를 비치, 운항하여야 한다. 이를 위해 선박마다의 고유식별번호(IMO번호)를 선체에 영구 표시토록 강제화하고 있으며 선박이력기록부를 선내에 의무적으로 비치하도록 하고 있으며 선종별 선박보안 경보장치를 탑재하고 보안증서 미소지 선박은 입항거부 또는 출항정지 등 국제항해가 불가능하도록 하고 있다.

항만시설부문에 있어서는 항만시설보안책임자를 임명하고 항만보안평가를 실시한 후 보안계획을 수립하여 당해국 정부의 승인을 받아야 한다. 보안계획 미 수립 항만에 기항한 선박 및 선적된 화물에 대하여는 외국항에서 별도 보안확인 절차 실시로 운항지체 등 피해가 발생할 우려가 있다.

각 국 정부는 자국의 선박, 항만의 보안계획 승인과 보안심사, 외국 선박에 대한 보안점검을 실시하고, IMO에 자국의 보안 관련 사항을 보고하여야 한다. 입항거부나 출항정지 등을 위한 명백한 근거(8가지) 발견 시 운항통제가 가능하도록 하고 있다.

ISPS Code는 특히 화물의 해상운송에 대한 보안을 확보하기 위한 국제협약으로 Part A와 Part B로 구분되어 있으며, Part A는 이행이 강제되는 사항을 Part B는 임의규정으로 구성되어 있다. ISPS Code는 국제항해에 종사하는 선박, 즉 고속여객선을 포함한 총톤수 500톤 이상의 고속 화물선, 이동식 해양구조물 및 국제항해에 종사하는 선박 및 관련된 항만시설이 적용대상이다. 하지만 관공선, 군함, 비상업용 목적의 정부 소유 선박은 적용이 제외된다.

당사국 정부의 책임은 보안등급 설정 및 보안선언, 보안관계 연락처 선정, 선박에 보안정보 제공, 항만내의 선박 또는 입항하려는 선박에 대한 통제, 항만시설 보안평가, 보안계획서 승인 및 선박보안심사, IMO에 필요사항 통보, 타 당사국과 상호 보안협정문 체결 등이다.[23]

2) 보안기준 주요 내용[24]

선박과 관련한 주요 규정은 보안선언서, 회사의 의무, 선박보안, 선박보안평가, 선박보안계획서, 기록, 회사보안책임자/선박보안책임자, 선박보안의 교육·훈련 및 연습, 선박의 심사 및 증서발급으로 나누어진다. 항만시설에 대해서도 유사한 규정을 적용하고 있는데, 항만시설보안, 항만시설보안평가, 항만시설보안계획서, 항만시설보안책임자, 항만시설에 관한 교육·훈련 및 연습이다.

특히 항만시설에 대한 보안평가는 보안의무의 이행, 항만시설에의 접근 통제, 항만시설의 모니터링, 제한구역의 모니터링, 화물취급 감독, 선용품 취급 감독, 보안통신의 유효성 보장 등을 검토하는 내용으로 구성되어 있다. 예로서 보안 2등급의 항만시설인 경우 항만시설에의 접근통제에 대한 보안 점검은 다음과 같다.

첫째, 보안2등급에서 접근지점이나 경계 장벽을 보호하는 인원을 추가로 할당하였는가?

둘째, 보안2등급에서 항만시설 접근지점의 수를 제한하는 조치를 수립하였는가?

셋째, 보안2등급에서 항만시설 접근지점을 통한 이동 저해조치를 수립하였는가?

---

23) 허윤석, “국제물류보안 강화에 따른 공급사슬 위험관리 및 지향성이 국제무역업체의 성과에 미치는 영향에 관한 연구”, 성균관대학교 석사학위논문, 2013.

24) 고현정, “우리나라 물류보안 인증제도 효율화 방안에 관한 연구”, 「로지스틱스연구」, 19(2), 2011, pp.65-85 ; 고현정, “국제물류보안 인증제도 동향 및 시사점에 관한 연구”, 「한국항만경제학회지」, 27(2), 2011, pp.333-354 재정리.

넷째, 보안2등급에서 인원, 휴대품 및 차량의 검색빈도를 증가하는 조치를 하였는가?

다섯째, 보안2등급에서 항만시설에 검증 가능한 정당성을 제시하지 못하는 방문자의 접근을 거부하였는가?

마지막으로 보안2등급에서 해상 보안을 강화하기 위한 순찰선을 사용하는 조치를 하였는가?

제3절 주요국의 해상공급사슬보안 인증제도

1. 미국의 C-TPAT

1) 개요[25]

미국은 2001년 9·11 테러 이후 테러용 무기가 미국으로 반입되는 것을 예방하는 동시에 국제화물 및 운송수단의 흐름을 촉진하고자 정부와 민간기업의 협력을 강화하는 물류보안 인증제도인 C-TPAT을 고안하였다. C-TPAT은 국제화물의 흐름에 참여하는 모든 주체 및 정부가 긴밀한 협조를 통해 최고의 보안을 확보할 수 있다는 인식에 기반을 두며, 국토안보부의 관세보호국(Customs and Border Protection)이 관리·운영하고 있다.

C-TPAT에는 수입업자, 국내운송업자, 선사, 항공사, 통관업자, 창고업자, 해외제조업자 등이 참여가능 하며, 이들 기업들은 세관과 민간업계가 공동 개발한 보안기준[5]인 시설 및 직원 보안, 교육과 훈련, 접근통제, 적하목록절차, 운송수단 보

25) 고현정, "국제물류보안 인증제도 동향 및 시사점에 관한 연구", 「한국항만경제학회지」, 27(2), 2011, pp.333-354 재정리.

안 등의 항목에 대해 종합적인 평가를 받게 된다.

C-TPAT은 인증등급을 3단계로 구분해서 운영되고 있는데, 등급마다 차등적인 통관 혜택을 부여하고 있다. 1단계는 프로그램 참여가 허용된 상태로 화물 검사회수가 축소되며, 2단계는 1단계의 혜택 외에도 화물의 우선적 검사기회 부여, 마지막으로 3단계는 화물검사 면제 이외에도 다양한 혜택을 부여받게 된다.

미국은 C-TPAT의 자국 내 활성화를 위해 특별한 정부지원은 제공하지 않지만, 기업이 인증을 위해 투자된 비용을 상쇄할 수 있는 실질적 통관혜택을 부여하겠다는 방향으로 추진하고 있다. 또한 보안기준의 현실성을 반영하기 위하여 산업계와 협의하여 보안기준을 개발하고, C-TPAT 프로그램을 효율적으로 운영하기 위해 C-TPAT 전문가 양성뿐만 아니라 데이터 및 정보관리 능력을 향상시키기 위해 노력하고 있는 것이 특징이라 할 수 있다.

2) 보안기준 주요 내용[26)]

C-TPAT은 업종별 특성에 따라 조금씩 상이한 보안기준을 적용하고 있으나 대부분 유사한 내용을 포함하고 있다. 보안기준은 8항목, 사업파트너 요구사항, 컨테이너 및 트레일러 보안, 접근통제, 직원보안, 절차보안, 물리적 보안, 정보기술 보안, 보안훈련 및 위협인지로 구성되어 있다. 이들 항목들은 업종별 특성에 따라 추가되기도 하고 면제되기도 한다.

첫째, 사업파트너 요구사항은 제조기업의 경우 부품/원료 공급업체, 운송업체, 중개인 등의 파트너와 연계되어 있는데, 사업 파트너를 선정 시 보안검증 절차를 적용해야 하는 내용이다. 즉, 사업파트너 사업현장에서의 출하, 제조, 조립 등의 활동에 대한 보안 무결성이 확보되어야 한다.

---

26) 고현정, 상게서, 2011, pp.333-354 재정리.

둘째, 컨테이너 및 트레일러 보안은 화물의 선적 장소에서 운송수단의 보안 무결성(integrity)을 확보하기 위하여 무권한(unauthorized) 물체 및 사람의 진입을 차단하는 절차를 마련해야 하는 내용이다. 이를 위해 ISO 17712 표준에 부합하는 봉인장치 이용, 보안이 확보된 장소에 컨테이너 및 트레일러 보관, 컨테이너의 내·외부 검사, 차량의 바닥・천정・뒷면 등을 검사해야 한다.

셋째, 접근통제는 기업이 운영하고 있는 각종 시설에 대한 무단진입을 방지하고 사원 및 방문자를 관리하는 절차를 마련하여 자산을 보호해야 하는 내용이다. 출입구에서 외부 방문자의 신원을 파악해야 한다.

넷째, 직원보안은 채용시 사원의 신원조사 체계를 마련하고, 보안장소에는 직무수행에 필요한 허가된 자만이 허용되어야 하고 신분증 발급과 취소 절차가 관리되어야 한다.

다섯째, 절차보안은 공급사슬에서 화물의 운송, 취급 및 보관 등과 관련된 절차들의 무결성 및 보안을 보장하는 절차를 마련해야 하는 내용이다. 화물 흐름과 병행하여 발생하는 모든 정보는 명확하고 정확히 관리되어야 하고, 그 정보를 보호하는 절차를 마련해야 한다. 즉 선적화물은 적하목록상의 정보와 일치하고, 중량, 라벨, 개수 등이 정확하게 표기되어야 한다.

여섯째, 물리적 보안은 화물취급 및 보관시설의 무단출입을 방지하는 물리적 장벽 및 무권한의 접근을 통제하는 체계를 구축해야 하는 내용이다. 즉 출입구, 주차지역, 건물 구조, 잠금장치 및 조명 등에 CCTV와 경고시스템을 구축하여 보안을 확보하는 치침을 마련해야 한다.

일곱째, 정보기술 보안은 무권한의 접근 및 조작으로부터 데이터를 보호하기 위한 정보기술의 무결성을 확보해야 하는 내용이다. 즉 자동화 시스템의 경우 규칙

적으로 암호변경을 하거나 개인은 자신의 계정만 사용하도록 하는 정보의 보안정책, 절차 및 표준을 마련하는 것이다. 또한 부적절한 출입, 조작, 데이터의 변조 등을 방지하는 시스템을 설치해야 한다.

여덟째, 보안교육 및 위협인지는 테러범 및 밀수업자가 가하는 위협을 인지하고 그 인식을 고취시키는 위협인식 프로그램을 확립하여 관리해야 하는 내용이다. 즉 직원들은 보안상황을 전달하고 보고하는 절차를 숙지하도록 해야 하는데, 화물의 선적 및 인수뿐만 아니라 우편물의 수취 및 개봉할 경우에도 보안 상황을 인식하도록 훈련을 받아야 한다.

2. EU의 AEO

1) 개요[27]

EU의 AEO는 Community Customs Code(CC)의 Article 5a와 Implementing Provisions(CCIP)의 Articles 14a-14q에 명시되어 있다.

AEO 가이드라인은 Part 1, Part 2, Part 3로 구성되어 있는데, Part 1은 일반적 사항 즉, AEO 심사와 혜택, 국제공급사슬 및 보안개념, AEO 지원서 제출지역, 감사에 대한 내용을 설명하고 있다. Part 2는 AEO 인증의 평가기준에 대한 설명과 각 평가기준에서 주요검토 사항을 언급하고 있다. 그리고 Part 3은 공급사슬에서의 활동주체 별, 즉 제조기업, 수출업자, 포워더, 창고 운영사, 운송사, 관세사, 수입업자 등이 AEO 인증 시 고려해야 할 평가항목을 설명하고 있다.

AEO 인증은 3가지 형태, 즉 AEO-관세절차 간소화, AEO-보안 및 안전, AEO-

27) 고현정, 상게서, 2011, pp.333-354 내용 참조하여 재인용.

관세 절차 간소화/보안 및 안전으로 구분되며 기업의 자발적인 참여에 따라 운영되고 있다.

AEO-관세절차 간소화는 관세행정 부분이 강조된 인증형태로 관세법 준수, 기록 및 보관 표준 마련, 재정능력의 기준을 통과한 조직에게 부여하는 인증이며, AEO-보안 및 안전은 관세절차 간소화 기준에 보안 및 안전 기준이 추가된 인증이다. 마지막으로 AEO-관세절차 간소화 및 보안 및 안전은 모든 AEO 혜택을 누리기 위해 취득하는 인증이다. 이러한 인증형태는 그 특성에 따라 상이한 통관혜택을 부여하고 있다.

AEO 프로그램에서 특별한 정부지원 사항은 언급되지 않고 있으며 다만 중소기업에 대한 특수상황을 고려하여 심사기준을 적용하도록 하고 있다. 정부의 재정적 지원보다 프로그램에 참여한 기업에게 다양한 통관혜택을 부여하고 있다. 특히 영국의 경우는 물리적 및 서류 검사의 축소, 우선통관, 통관서류 간소화, EU 지역에서의 인증부여, BSKM자격[28]을 부여하여 기업경쟁력 강화지원, BSKM의 글로벌 인지도 지원, 미국 등과의 타 국가와의 상호인증 참여, 운송 보험료의 감소 등의 혜택을 부여하고 있다.

2) 인증기준 주요 내용[29]

EU의 AEO 인증을 위한 평가기준은 5가지 영역, 즉 기업정보, 법규준수 기록, 기업 회계 및 물류시스템, 재정능력, 안전 및 보안요구로 구성되어 있다. 특히 평가 항목가운데 안전 및 보안요구와 기업회계 및 물류시스템 영역에서 기업이 물류보안 국제인증인 ISO 28000, ISPS Code[30], TAPA[31]인증을 보유한 경우 AEO 인

28) BSKM : British Standards Kite Mark.

29) 고현정, 상게서, 2011, pp.333-354 내용 참조하여 재인용.

30) ISPS Code : International Code for the Security of Ships and Port Facilities.

증 심사에서 동일 평가 항목에 대하여 중복심사를 가능한 축소하여 심사 효율성을 추구하려는 부분이 특징이라 할 수 있다.

첫째, 기업정보 영역은 기업규모와 관세 관련 통계에 관한 항목을 포함한다. 기업 규모는 과거 3년 동안의 매출액 및 손익, 보관능력, 구매량, 생산품, 판매량 등에 관한 정보를 의미한다. 또한 관세 관련 통계는 품목분류, 수입관세 비율, 소비세 등과 관련된 정보이다.

둘째, 법규준수 기록은 세관법과 타 법규준수에 관한 내용으로 세관거래, 세관 관련법 및 법규 준수에 관한 평가항목이다.

셋째, 기업회계 및 물류시스템은 감사(audit), 회계시스템, 생산운영 관련 내부 통제시스템, 제품흐름, 통관절차, 정보보안(전산시스템, 문서 등)에 관한 사항으로 투명한 회계정보와 세관과 기업간의 원활한 정보 공유 부분을 평가하는 항목이다. 넷째, 재정능력은 보안시스템을 포함하여 기업이 정상적으로 운영될 수 있는 재정적 능력의 유무를 판단하기 위한 항목이다.

마지막으로 안전 및 보안요구는 크게 자체보안평가, 출입통제, 물리적 보안, 화물취급, 비즈니스 파트너보안, 인력보안 및 외부서비스로 구분할 수 있다. 자체보안평가는 기업 자체적으로 자사와 관련된 공급사슬에서 발생할 수 있는 위험 및 위협을 식별하고 이에 대한 조치를 기업 스스로 평가한 산출물을 의미한다. 출입통제는 작업장, 적재 및 선적장소에 대한 무권한 차량 및 사람의 접근을 통제하고, 불법 침입이 발생할 경우 이에 대한 적적한 조치를 마련하는 하는 것을 의미한다. 물리적 보안은 빌딩 및 출입구, 잠금장치, 외부경계 울타리, 경고시스템, CCTV를 설치하여 각종 시설에 대한 불법 침입을 통제하는 조치를 평가하는 것이다. 화물취급은 화물 흐름에서 물품의 손실, 교체, 변경에 대한 부정수단의 접근을 방지하

31) TAPA : Technology Asset Protection Association Certificate.

는 조치를 마련하는 것이다. 이러한 조치는 화물단위[32], 물류절차, NFR[33], 물품반입, 물품저장, 물품생산, 물품적재 등을 대상으로 한다. 비즈니스 파트너보안은 자사와 연계한 국내외 비즈니스 파트너의 대한 신분증명을 위한 조치를 마련하는 내용이다. 즉 국내외 비즈니스 파트너 선정 시 해당 업체에 대한 보안상황을 점검하고 지속적으로 점검하는 절차를 마련해야 한다는 것이다.

AEO제도의 도입의의는 국제관세기구 (WCO) 국제표준규범을 이행하는 것으로, 테러, 마약 등 불법물품의 반입을 차단해 사회 안전과 국민건강을 보호하고, 신무역장벽인 '수출입 안전' 장벽을 극복해 기업의 국제 경쟁력을 제고하는 생존전략이며, 또한 기업관리를 통한 선제적 위험관리를 통해 관세행정 및 조직의 효율적 운영을 도모하는데 있다. AEO제도의 도입 의의에 대해서 살펴보면 다음과 같다.[34]

기업측면에서의 AEO제도의의는 첫째로 국제적으로 안정성과 신뢰성을 인정받는 기업으로 통용돼 거래선 확보와 경쟁력 향상을 통해 기업의 이미지 가치가 상승되는 효과가 있다.

둘째로 AEO인증업체는 검사비율 하향, 신용담보액 상향 조정 및 신고방법 간소화 등의 관세행정상의 특별한 혜택을 받게 됨으로써 세관과 수출입 관련 고객과의 유대관계를 돈독히 할 수 있다.

셋째로 AEO제도는 AEO국가간 상호인정협정(MRA) 체결을 통해, 자국에서 인증받은 AEO인증업체가 상대국 세관에서도 자국에서와 동일한 통관상의 혜택을 수혜하게 됨으로써 검사축소, 신속통관 및 절차 간소화 등의 혜택을 받아 통관비용 및 시간에 있어 수출경쟁력의 향상을 기할 수 있다.

---

32) 화물단위는 화물 운송에 사용되는 컨테이너, 탱커, 벤, 화물자동차, 운송기기, 파이프라인 등을 의미한다.

33) NFR은 Non-Fiscal Requirement로 수출입 금지 또는 제한품목에 대해 허가유무와 이중사용 물품을 거래유무, 통상금지 물품의 거래 유무를 의미한다.

34) 광양관세사 홈페이지 참조(http://www.kyca.co.kr)하여 내용 정리.

넷째로 물류공급망에 있는 주요업체는 앞으로 국내외 AEO 인증업체와 거래하기 위해서는 반드시 AEO 인증업체가 돼야만 거래관계가 성립될 수 있게 됨에 따라 AEO 인증은 물류공급망에 관련된 업체의 생존전략이 될 것이다.

그리하여 관세청은 주요관세행정을 AEO제도와 접목하기 위해 AEO공인업체의 사후관리 개념으로 기존 종합심사제도를 통합 운영하게 되며, 모든 기업체에 대한 평가 기준을 종합심사보다 포괄적인 AEO기준으로 통합해 적용하게 되고, AEO 연착륙 지원을 위해 현행의 관세행정상 통관, 납세절차 특례규정을 재정비해 AEO 평가결과에 비례한 혜택을 부여해, 자율적 참여를 유도하기 위한 최대한의 혜택을 부여하되, 업체의 충격을 최소화하기 위해 순차적으로 적용하게 되며, 앞으로의 관세행정의 주안점은 비AEO 공인업체를 중심으로 이뤄지게 되어 있다.

그러므로 물류공급망에 있는 수출·입업체·관세사·화물운송주선업자·보세운송업자·보세구역운영인·선박회사·항공사·하역업자 및 자유무역지역 업주 기업체 등은 AEO 인증을 받기 위해 최대한 노력을 경주해야 할 입장에 있다 하겠다.

현재 AEO 시범사업을 거쳐 현재 삼성전자 등 9개 업체가 AEO업체로 인증돼 있고, 현실을 고려한 업종별 공인기준의 세부 가이드라인을 작성 중에 있으며, 공인업체에 대한 가시적 혜택을 마련하기 위해 관련업계와 계속 협의하고 있다.

끝으로 가능한 많은 업체가 AEO로 공인받게 하기 위해서는 중소기업에 대한 심사기준의 완화 내지 탄력적 운영이 필요하다고 사료되고, 주요국과의 AEO 상호인정협정이 신속히 체결되어야 할 것이다.

3. 싱가포르의 STP

1) 개요[35]

싱가포르 세관은 2007년 글로벌 공급사슬 보안확보와 원활한 상거래를 위해 STP(Secure Trade Partnership)라는 자발적인 참여 방식의 보안인증 프로그램을 마련하였다. STP에는 STP와 STP-Plus라는 두 가지 형태의 인증을 운영하고 있는데, STP-Plus는 STP 보다 한층 더 높은 보안기준을 갖춘 기업에게 부여되는 인증이다.[36]

이에 따라 모든 기업이 자사의 환경에 적합한 인증에 참여할 수 있도록 유도함으로써 싱가포르는 국제적으로 보안 허브라는 이미지 확보를 추구하고 있다.

싱가포르는 공급사슬보안의 중요성 인식 및 STP 프로그램 확산을 위해 무료 STP 과정 운영, 일대일 기업컨설팅 등의 다양한 프로그램을 운영하고 있다.[37] 기업지원은 세관과 타 기관, 즉 EDB[38](Economic Development Board) 또는 SPRING Singapore[39]와 협력하여 사업을 운영하고 있다. EDB는 Initiative in New Technology라는 제도를 활용하여 공급사슬보안 시스템 구축 시 보조금을 지원하고, SPRING Singapore는 LCDP(Logistics Capability Development Program)를 통해 중소물류기업의 보조금 지원, SIP[40]를 통한 재정적 지원, CMC[41]를 통한

35) 고현정, "국제물류보안 인증제도 동향 및 시사점에 관한 연구", 「한국항만경제학회지」, 27(2), 2011, pp.333-354 재정리.

36) 국제물류보안 동향과 인증제도 비교(웹사이트 참조 : http://sekujung.blog.me).

37) 한국교통연구원 화물운송시장정보센터, 물류브리프, 참조

38) EDB는 싱가포르를 글로벌 비즈니스 허브로 성장시키기 위해 운영되는 정부기관으로 해외투자 유치, 신성장 산업 발굴 및 경쟁력 강화, 우호적 기업환 조성 등의 사업을 추진하고 있다.

39) SPRING Singapore는 혁신기업과 경쟁력 있는 중소기업을 육성하기 위한 기업발전 지원 정부기관이며, 주요 업무로는 기업에게 재정, 경영능력 향상, 기술 및 혁신, 시장진출 등을 지원하는 것이다. 또한 국가표준기구로써 국제표준과 품질보증의 개발· 촉진 업무와 국가경쟁
력강화 및 무역촉진 등의 업무를 수행한다.

컨설팅 및 인증비용 지원 등을 제공하고 있다.[42]

2) 인증기준 주요 내용

STP Guidelines과 STP Criteria는 각각 STP와 STP-Plus 인증을 받는데 적용되는 인증기준이다. 특히 STP-Plus는 타국과의 상호협정에서 국제적 보안기준을 충족한 기업으로 인증하고 있다. STP 또는 Plus 프로그램에 참여한 기업들이 갖추어야 할 보안 요구사항은 보안관리시스템 구축, 리스크평가, 보안기준 등이며 세부적인 내용은 다음과 같다.

보안관리시스템 구축은 기업의 보안정책 및 목적설정과 피드백 수 있는 체계, 기업 내 효과적인 의사소통 절차, 지속적으로 보안 적합성 및 개선 절차를 개발하고, 이를 문서화하고 이행·유지·검토하는 시스템을 의미한다. 리스크평가는 기업의 비즈니스 유형에 적합한 자사 내부의 운영프로세스와 자사와 연계된 공급사슬리스크에 대한 평가를 실시해야 한다. 이 평가를 통해 공급사슬 측면에서 자사의 리스크와 취약요소를 줄이도록 해야 하는데, 그 대상으로 제조업자 및 공급업자, 창고 관리자 및 소유주, 운송업자, 터미널 운영사, 해상 및 항공 운송업자 등을 포함한다.

보안기준은 기업들이 준수해야 할 8가지 항목을 규정하고 있는데, 그 항목은 시설보안과 접근통제, 인력보안, 비즈니스 파트너보안, 화물보안, 운송보안, 정보 및 정보기술 보안, 사고관리와 조사, 리스크 관리와 사고수습이다.

---

40) SIP(Standards Implementation for Productivity)은 SPRING Singapore에서 제조업 및 서비스 분야의 생산성 향상을 위해 표준(standards)의 도입을 지원하는 사업이다. 주요 효과로는 생산성/품질/고객만족 향상, 효율성 향상, 자동화를 통한 휴먼 에러 감소, 생산비 절감 등이다.

41) ISO 28000을 도입하는 기업이 참여하는 프로그램으로 고객, 공급자, 운송사 등 적어도 3개의 기업이 참여해야 하며, 이들 기업 가운데 반드시 중소기업이 참여해야 한다. 인건비 및 전문가 서비스 관련 비용의 70%, ISO 28000 인증비용의 최고 30%를 지원한다.

42) 항만물류안전의 확보를 위한 보안제도에 관한 고찰(웹페이지: http://www.hanyang.ac.kr)참조.

첫째, 시설보안과 접근 통제는 담장(wall or fence)을 적소에 설치하여 기업 시설물에 대한 내외부의 무단 침입을 방지해야 한다는 내용이다.

둘째, 인력보안은 직원의 신원조사를 위한 절차를 마련하고, 직원이 보안과 보안위협에 대한 행동대책을 숙지하도록 하는 절차를 마련하는 것이다.

셋째, 비즈니스 파트너 보안은 기업은 글로벌 공급사슬 보안향상을 위해 비즈니스 파트너의 자발적인 보안기준 강화를 유도하고 협력해야 한다는 내용이다.

넷째, 화물보안은 인가받지 않은 물질 및 개인의 침투를 방지하기 위해 화물의 무결성을 확보하는 절차를 마련해야 한다는 것이다.

다섯째, 운송보안은 권한 없는 사람이나 물질의 침입을 방지하기 위한 운송수단(트럭, 트레일러 등)에 대한 보안 절차를 마련해야 하는 것이다.

여섯째, 정보 및 정보기술 보안은 정보의 오용 및 변경을 포함해서 공급사슬에서 사용된 데이터와 정보시스템의 기밀성 및 무결성을 유지하기 위한 절차를 마련하는 것이다.

일곱째, 사건관리 및 조사는 사건 또는 위기 상황에 대한 체계적인 대응책과 그 발생의 근본원인을 파악하여 재발 방지를 위한 절차를 마련하는 것이다.

여덟째, 위기관리 및 사건복원은 사고나 보안사건의 영향을 최소화하기 위한 위기관리 및 복원 절차를 마련하는 것으로 그 절차는 특수한 상황에서의 사전 계획과 운영 프로세스 수립을 포함해야 한다.[43]

43) 전략물자관리원, “연례보고서”, 2010 참조.

4. TAPA[44)]

오늘날 공급망(Supply Chain) 안에서 관련 기관과 업체간 IT를 활용한 정보교환의 중요성이 부각되고 있는 것은 이를 통해 분실 및 도난사고의 가능성을 최소화 시킬 수 있을 뿐만 아니라 고객지향적 서비스 제공능력을 향상시킬 수 있기 때문이다. Supply Chain 흐름에 있어서 Security를 보장하지 못하면 SCM(Supply Chain Management : 공급망 관리)은 공염불에 불과할 것이다.

SCM에서 화물의 보안을 구축하는 방법은 두가지 측면[45)], 즉 Software적인 면과 Hardware적인 면에서 접근할 수 있겠다. Software적인 면은, 화물에 대한 자세한 정보를 사전에 확보하여 보안을 강화하는 것이다. 고객이 물건을 발송하기 위해 작성하는 상업송장이나 운송업자들이 세관에 제출하는 적하목록(Manifest)등을 예로 들 수 있는데, 화물보안의 선결조건은 각 주체들이 성실하고 정확하게 화물의 정보를 제공하는 것이다. 이는 최근 미국세관이 해상화물의 경우는 입항 24시간 이전, 항공화물은 4시간 이전에 관련 화물의 정보를 요청하는 것과 맥락을 같이 한다고 볼 수 있다. 보안강화를 위한 Hardware적인 부분은 전자봉인시스템, 실시간 위치 추적이 가능한 RF Chip (Radio Frequency Chip : 각 화물에 고유 식별번호가 내장된 컴퓨터 칩을 부착하여 전 세계 어디서든지 인공위성에 의해 추적이 가능 하도록 하는 것) 등을 들 수 있다.

첨단 하이테크 및 고가의 제품을 생산하던 업체들은 더 이상 기존 운송 서비스 업체들의 취약한 보안시스템에 의지하지 않고, 자신들이 보관 및 운송과정에 있어서 자사의 제품을 직접 보호하겠다고 발 벗고 나서게 되었다. 1997년 7월 미국의 컴팩, 선 마이크로 시스템즈, 인텔이 주도하여 보안전문가들을 포함한 35명이 화물

44) 기술자산 보호협회(http://korean.jupiterexp.com) 홈페이지 참조하여 재정리.

45) 성낙청, “AEO 공인 제도의 D사 적용 방안을 중심으로”, 서경대학교 석사학위논문, 2011. 참조하여요약

안전운송 보안기준을 제시하였고 그들의 기준에 적합한 운송업체들에게 자사의 물류부분을 맡김으로써 화물의 보안을 강화할 수 있었는데 이것이 기술자산보호협회(Technology Asset Protection Association : TAPA)라는 조직의 결성 배경이다.

성낙청(2011)의 연구에 의하면, “TAPA는 TAPA US, TAPA EMEA (Europe, Middle East and Africa), TAPA Asia의 3대 지역별 조직으로 운영되고 있으며, 그 중 TAPA Asia는 2000년에 여러 전자제품 및 반도체 제조업체, 하이테크 산업, 운송업체 및 관련 보안 전문컨설팅 업체가 함께 모여 조직한 비영리 보안 전문 기관으로 현재 총 60개 회원사의 181명이 등록되어 있으며 그 회원들에게 첨단 하이테크 제품의 취급 및 운송과 관련된 보안절차 등을 안내하고, 여러 가지 관련 정보를 공유함으로써 예상치 못한 문제를 사전에 예방하고, 문제 발생 시 신속하게 대응하도록 함으로써 문제의 확대를 최소화하기 위한 노력을 도모”하고 있다.

제4장 해상공급사슬보안과 위험관리 전략

제1절 해운기업의 해상공급사슬보안 활동

1. 해운기업의 해상공급사슬보안 요소 및 범위[46)]

공급사슬 보안은 개별기업의 노력만으로 그 효과를 충분히 발휘하기 어렵다. 공급사슬상의 모든 활동은 서로 연계되어 개별기업 차원에서 확고한 보안시스템을 구축하였더라도 공급 네트워크를 구성하는 여러 단계 중 어느 한 곳이라도 보안상의 허점이 발생하는 경우에는 공급사슬 전체가 보안위험에 노출되게 된다. 따라서 물류보안은 개별기업 차원이 아닌 전체 공급사슬 네트워크의 관점에서 다루어져야 한다.

보안위험은 여러 요인들의 상호작용에 의해 야기된다. 가령, 컨테이너는 밀수, 불법이민, 대량살상무기의 밀반입 등에 이용될 가능성이 높다. 컨테이너 선박, 자체가 테러공격의 대상이 될 수 있으며, 테러공격을 위한 무기나 수단으로 이용될 수 있다. 선박의 등록 및 소유관계에 있어서 투명성의 결여는 테러리스트들이 선박을 범죄적인 목적에 악용할 수 있는 소지를 제공한다는 점에서 보안위험을 초래할 가능성이 있다.[47)] 컨테이너 운송은 전체 공급사슬 활동 중 일부 영역에 지나지 않는다. 도로 및 철도, 항공운송을 비롯하여 항만이나 공항설비 등 물리적 시설 등도 보안위협으로부터 자유로울 수 없다. 생산, 운송, 보관, 하역에 관여하는 공급사슬 당사자들 역시 테러행위에 직접 혹은 간접적으로 개입할 수 있다는 점에서 공

---

46) 양정호, “글로벌 기업의 공급사슬보안 및 위험관리전략에 관한 연구”, 「경영과 정보연구」, 27, 2008, pp.149-172 참조하여 재정리

47) 2003년 기준으로 약 5400대의 상선이 약 6만개의 항구에 기항하고 국제적으로 거래되는 화물의 90% 가량이 해상컨테이너를 이용한다. 그 중 약 2% 정도만이 목적지에 도착한 후 물리적인 검사를 받는다고 한다.(M. Van de Voort, et al., Improving The Security of the Global Sea-Container Shipping System, RAND Europe Report, MR-1695-JRC, 2003)

급사슬보안의 주요 대상이 된다. 따라서 기업들은 공급사슬 파트너 및 정부기관과 함께 물품의 입고에서 운송과정을 거쳐 소비자의 손에 인도되기까지 공급사슬상의 모든 지점에서 보안사항을 감시하고 안전을 확보하기 위해 상호 협력해야 한다.[48]

Hamilton[49]은 계획에서부터 실행 및 통제에 이르기까지 모든 단계에서 핵심적인 역할을 수행하는 것은 인간이기 때문에 기술적인 요소에만 의존하여서는 결코 효과적인 보안을 달성할 수 없다고 한다. Wiederin[50]은 일련의 과정, 정책, 절차 및 인적요소, 그리고 최신 보안기술이 상호 작용하여 완전한 보안을 제공한다고 한다. 이렇듯 효과적인 보안관리를 위해서는 내부와 외부의 다양한 영역과 위험요소들을 고려하는 전체적이고 포괄적이며 통합적인 접근방식을 요한다.[51]

한편, 공급사슬상 어느 한 지점에서 보안상의 문제가 발생하면 그 효과는 공급사슬 전체로 확산될 수 있다. 따라서 공급사슬상 어느 단계에서 발생한 보안상의 결함을 그 다음 단계에서 방어할 수 있도록 보안시스템을 계층적으로 유지할 필요가 있다. 여러 보안기능들이 복합적으로 연결되어 상호 지원해주는 다중 보안시스템은 개별 보안요소가 그 기능을 완벽하게 수행하지 못하더라도 다른 요소들을 통해 그 결함을 보완할 수 있기 때문에 어느 단일 계층에서 보안상의 허점이 발생하더라도 그로 인하여 보안시스템 전체가 붕괴되지는 않으며, 테러행위를 지연시키거나 그 효과를 경감시키는 효과가 있다.[52]

---

48) Ravi Sarathy op. cit., p.31.

49) CR. Hamilton, The case for holistic security: The integration of information and physical security as an element of homeland security, 2004(www.riskwatch.com/Press/Holistic_Security_10-03.pdf)

50) S. Wiederin, D. Wurster, RS Hoefelmeyer and T. Phillips, The true meaning of security, 2002 (www.rrtidd.com/webQuest/shared/true%20Meaning%20of%20Security.pdf)

51) Vinh V Thai & Devinder Grewal, The Maritime Security Management System: Perceptions of the international Shipping Community, Maritime Economics & Logistics, 2007. 9., p.129.

1) 생산장소

생산장소에서 발생하는 보안문제는 제품의 부당한 변경(tampering) 혹은 대체(substitution)가능성 등으로 이는 고객의 불만을 야기하고 신제품의 출시나 제품의 가용성을 지연시키거나 방해하는 한편, 기업의 책임 및 평판에도 영향을 미칠 수 있다. 생산하도급자와 같은 조달파트너와 관련하여 채용과정에서의 면밀한 심사를 하고 제조설비에 대한 접근통제절차를 확립하며, 보안사항의 위반을 막기 위한 제조공정의 심사뿐만 아니라 파트너와의 신뢰관계를 구축하는 조치들은 보안사고로 인한 공급사슬의 혼란을 경감하는데 도움이 된다.

2) 제품

제품과 관련된 보안의 문제는 제품의 컨테이너 적재과정 감시, 컨테이너 적입 후 봉인 등의 과정을 통한 컨테이너의 무결성 확보, 운송 중 컨테이너에 적입된 내용물의 변경시도 감시, 도착 후 컨테이너의 무결성 검증 등이다. 컨테이너 봉인과 컨테이너에 부착된 센서와 같은 신기술은 운송 중 컨테이너화물의 변경을 제어하는데 도움이 된다.

3) 공급사슬 파트너 및 중개업자

C-TPAT와 같은 보안프로그램은 공급사슬 당사자들이 보안관행을 공유하도록 함으로써 공급사슬 보안의 표준을 설정하고, 보안규정의 준수를 점검하며, 이를 통해 신속절차와 같은 인센티브를 제공한다.

---

52) Making the Nation Safer - The Role of Science and Technology in Countering Terrorism Committee on Science and Technology for Countering Terrorism of the National Research Council, The National Academies Press, 2002, p.214.

4) 운송노드 및 운송인

화물보안을 위해서는 센서, 엑스선, 감마선, 방사능 감시, 자기장을 이용한 침입탐지 등의 보안기술들을 활용한 컨테이너 화물의 적격심사와 의심대상 컨테이너화물을 선별하여 현물검사를 실시할 필요가 있다. 컨테이너 적격심사의 목적은 핵물질이나 화학무기와 같은 위험화물을 검사하기 위한 것이다. 항만보안은 관찰뿐만 아니라 이미지를 수집하고 분석하며 위협을 탐지할 수 있는 고정 혹은 이동식 카메라로 이루어진 지능형 영상(intelligent vision)을 통한 감독과 함께 접근통제를 통해 이루어진다.

5) 인력

공급사슬의 매 단계마다 인력이 개입되기 때문에 공급사슬에 참여하는 모든 개별 당사자들의 신원을 보장하기 위한 보안조치들이 필요하다. 이는 선적전 송하인의 점검에서부터 적재 및 출하 단계에 개입하는 당사자들, 그리고 컨테이너 화물에 접근하는 당사자들의 감시에 이르기까지 포괄적인 보안조치가 필요하다. 다만, 개별 당사자들의 프라이버시와 정치적인 고려가 균형을 이루어야 한다.

6) 정보보안

공급사슬의 안정성 및 성과는 정확한 공급사슬정보의 확보 및 처리에 의존한다. 정보보안의 목적은 공급사슬정보에 대한 접근을 통제함으로써 정보의 위조 및 변조를 방지하고 공급사슬 정보의 기밀성을 높이는데 있다. 최근 정보보안을 위해 활용되고 있는 RFID 태그와 관련한 문제는 RFID 태그에 저장된 정보를 삭제하고 변경하는 해킹시도를 어떻게 방지할 것인가 하는 것이다. RFID 태그의 무결성이 확보되지 못하는 경우 태그에 저장된 정보의 신뢰성이 떨어져 RFID 태그를 활용한 정보보안의 효력이 상실되게 된다.

7) 공급사슬보안 활동 유형

공급사슬 내에 있는 조직은 공급사슬보안을 시행하기 위해서는 다양한 형태의 보안 활동을 수행하여야 한다. 보안 활동은 조직의 업무 특성 및 주변 환경 등에 따라 달라질 수 있으므로 각 조직은 각자의 특성에 적합한 보안 활동을 계획하고 실행하는 것이 필요하다. 서상범 외(2009)는 보안 활동을 물리보안, 정보보안, 인적보안, 절차보안 그리고 보안 기본 인프라 5가지로 크게 분류하고, 5가지 대분류 하위에 12개의 소분류를 구성하여 제시하고 있다. 이에 대한 것은 <표 4-1>에 제시되어 있다.[53]

<표 4-1> 공급사슬보안 표준 매뉴얼 보안유형 구성

Level 1	Level 2	보안활동 유형
물리보안 (투자관련 하드웨어 구성)	물리적 보안	화물 또는 물류시설 보호 및 감시를 위한 물리적 시설(펜스, 조명, 게이트, CCTV, 건물, 시건장치 등)
	접근통제	인가된 인력·차량에게만 접근을 통제(허가)하기 위한 시설
	공급사슬 운송 (Conveyance) 보안	운송장비(컨테이너, 트레일러, 팔레트) 관련 보안 장비
정보보안	접근 보안	정보시스템에 대한 선별적 접근 관리(패스워드 등) 보안활동
	데이터 및 정보 보안	데이터 및 정보 관리와 관련된 보안활동
인적보안	인원/종사자 보안	고용시 신원 확인 또는 해고(계약해지)시 기밀유지 등
	인원접근통제	인원의 시설(화물) 접근 허가 또는 거부 절차 수립, 인원에 따른 차별적인 접근 권한 설정 등
	보안교육 및 훈련	보안에 대한 교육 및 훈련관련 사항
절차보안 및 사후대비	문서/기록(Manifest) 관련 (절차) 보안	적하목록, B/L 등 화물 수령 및 배성 시 필요 정보가 서류상에 기재되었는지 여부 확인
	화물취급 절차 (Procedural) 보안	공급사슬 상 제품의 입증 가능한 위치를 알려주고 기록하는 과정에 대한 보안사항
	위기관리/비상 상황 극복계획	(공급사슬)보안 위해사태시 위기관리 및 재해복구에 관한 절차
보안 기본 인프라	거래당사자에 대한 보안 관련 요구	물류프로세스 내의 비즈니스 파트너에 대한 보안사항 점검 (위에서 정의한 물리, 정보, 인적, 절차 보안에 대한 점검과 유사 혹은 상시 커뮤니케이션 상태 파악)

자료 : 김영균, “항만터미널의 유형과 공급사슬보안경영 활동이 경영성과에 미친는 영향에 관한 연구”, 한국해양대학교 박사학위논문, 2011.

53) 서상범 외, “국가물류보안체제 고도화를 위한 물류보안표준참조모델 구축”, 「물류학학회지」, 제19권, 제2호, 2009, p.82.

황의찬 외(2009)는 항만터미널에 적용하기 위한 보안 활동을 시설관리, 화물관리, 직원관리 및 위기대응, 정보/통신관리 4가지로 크게 분류하고, 4가지 대분류 하위에 10개의 소분류를 구성하여 제시하고 있다. 이에 대한 것은 <표 4-2>에 제시되어 있다.[54]

<표 4-2> 항만터미널의 보안 활동 유형

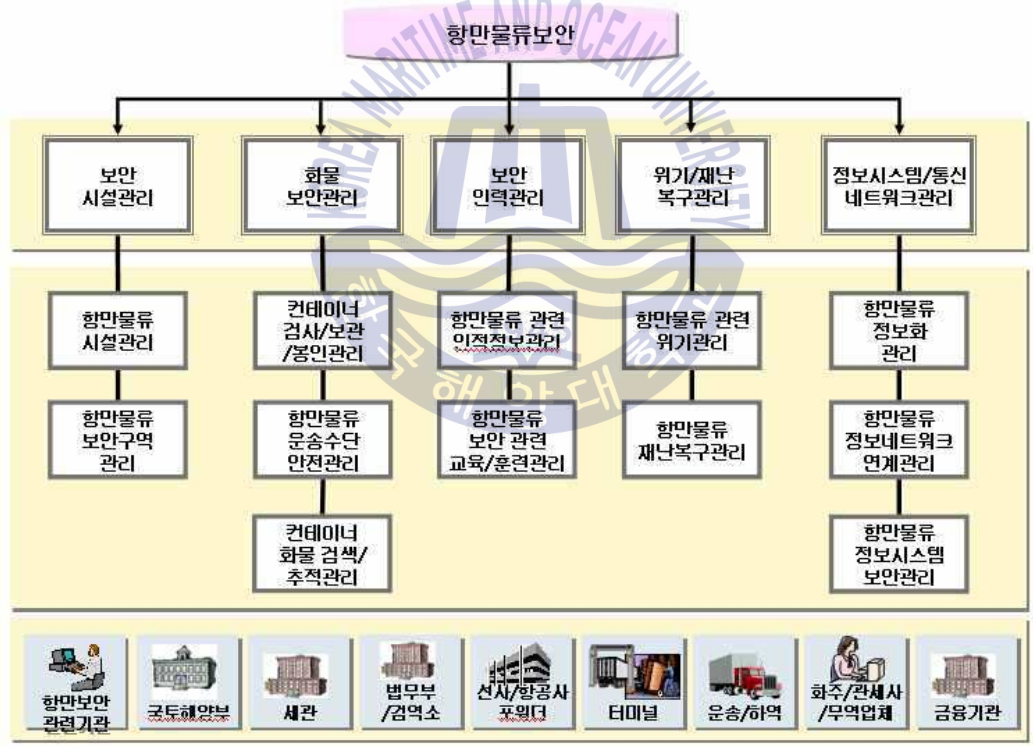
대분류	세부항목	내 용
시설관리	시설보호	- 시설물구조 및 안전-보안장비, 출입구 모니터링 - 입구, 출구, 화물처리/저장 지역, 보안울타리 - 잠금장치, 조명 설치, 경고 시스템
	보안구역 접근통제	- 업무 수행을 위해 필요한 영역에 대한 접근만을 허용 - 무권한자/비확인 개인의 확인·조사·취급절차 마련 - 피고용인, 방문자 신분 확인, 선박 방문자 일지 준비
화물관리	컨테이너 검사, 보관, 봉인	- 컨테이너에 대해 미승인 물체/사람의 침입 보호 유지 - 보안봉인 장착 공 컨테이너 검사 - 컨테이너를 안전한 영역에 관리/보관
	화물운송절차 및 운송수단 안전	- 화물 통제 및 반출절차 마련, 운송/하역 보안 절차 마련 - 운송기기 보안규정 마련, 출항 전 선박보안 점검 - 불법적/의심스러운 행동 탐지 시 세관 등에 통보
	화물검색과 추적	- 선박에 적재되기 전에 위험성 여부를 검사장비를 통해 신속 검사 - 이동 중인 화물의 위치 추적 - 위험화물 판단 시 적절한 조치
직원관리 및 위기대응	채용 및 직원정보 관리	- 직원 채용 전 경력 및 참조사항 등의 정보 검증 - 직원 채용 후 주기적 체크 및 재조사 - 직원 채용 종결 후 직원 신분증 해지 절차, 시설 및 시스템 접근 배제
	보안교육/훈련	- 직원 및 피고용인(필요한 경우 거래 파트너 포함) 보안교육 - 작업장, 운송기기 등에 대한 검사방법 훈련 - 보안인식 프로그램, 보안인증 자격증
	상황 발생 시 사고복구 능력 및 자기평가	- 비상사태 및 테러에 따른 복구절차 수립 - 보안위험 정기적 자기평가 서류화 및 수행(self risk assessment) - 평가결과 검토 및 피드백
정보/통신관리	정부 및 사업파트너와의 정보공유/협력	- 화물적화목록 정보 제공, 정부(세관)와 정보 교환 - 국제 승객 및 선원과 관련된 정보 명확하게 파악 - 화물 적하목록 기재, 정보가 정확하게 반영되었다는 보장절차 마련
	정보보안을 위한 통신방화벽 및 접근통제	- 데이터 관리, 기업 및 개인 정보 관리 - 패스워드, 방화벽 관리 - 정보 변경 및 오류 예방

자료 : 김영균, “항만터미널의 유형과 공급사슬보안경영 활동이 경영성과에 미친는 영향에 관한 연구”, 한국해양대학교 박사학위논문, 2011.

54) 황의찬 외, 전게서, pp.7-8.

김수엽(2009)은 물류보안에 대하여 국가 물류체계 내부 및 외부(요인)의 의도적인 위해 행위를 사전에 방지하거나 또는 위해 사태 발생 시 신속한 사후복구조치를 수행함으로써 안전하고 원활한 국가 물류체계를 확보하는 일체의 활동을 말하는 것으로 정의하고 있다. 또한 항만물류보안이란 내륙지역(육상)에서 수행되는 물류활동에 대한 보안(항공 및 해상물류와 병렬적인 공간 개념, Inland Logistics Security, 내륙에서 국경이 인접된 국가의 경우에는 일부 국제물류 활동까지 포함됨)과 국제(세관, 수출입 등) 물류 활동에 포함되는 모든 물류활동에 대한 보안이라고 정의하고 있다. 항만물류보안에 대한 개념은 <그림 4-1>에 제시되어 있다.[55]

<그림 4-1> 항만물류보안 개념도



55) 김수엽, “항만물류보안산업의 발전방안 연구”, 한국해양수산개발원, 2009, p.15.

2. 해운기업의 보안위험의 예방

공급사슬 보안시스템을 구축함에 있어서 최대의 쟁점은 공급사슬의 효율성을 그대로 유지하면서 보안사고를 효과적으로 예방할 수 있는 방법을 모색하는 것이다. 이에 대하여 전사적 품질관리(TQM: Total Quality Management)의 원리를 적용하면 보안사고를 예방하고 그 효과를 경감하는 동시에 공급사슬의 효율을 높일 수 있다고 한다.[56]

전사적 품질관리는 제품품질개선의 중심이 검사에서 예방으로 발전한 것으로 많은 기업들은 교육, 조직 전체의 협업, 설계개선, 공정변동 축소 등의 과정을 통해 검사비용과 제품의 하자를 획기적으로 줄이고 생산효율을 그대로 유지하면서 품질을 개선하는 것이 가능하다는 것을 경험하고 있다. 이러한 원리는 공급사슬관리에 적용되어 공급사슬상 보안위험을 줄이는 동시에 공급사슬의 효율을 높일 수 있는 대안을 제시할 수 있다.

9.11 테러사건 이후 수입화물에 대한 전수검사를 실시하자는 의견도 제기될 정도로 보안에 대한 관심이 높다. 그러나 이러한 문제해결방식은 검사비용을 증가시키고, 물류정체를 심화시켜 물류시스템의 효율을 떨어뜨리고 공급사슬을 불안정하게 만든다. 이는 결국 재고비용을 증가시키고 화주 및 고객에 대한 서비스 수준을 떨어뜨리는 등 공급사슬 전반에 걸쳐 부정적인 영향을 미칠 수 있다.

전사적 품질관리의 관점에서 공급사슬보안은 보안사고 발생으로 인한 혼란을 수습하기 위한 대책을 강구하는 차원에서 논의되기 보다는 공급사슬상 보안위협을 사전에 탐지하고 이에 신속하게 대응함으로써 보안사건을 미연에 예방하고 영향을 최소화할 수 있는 시스템을 구축해야 할 것이다. 가령, 검사비율을 늘리기 보다는

---

56) Hau L. Lee and Michael Wolfe, “Supply Chain Security without Tears”, SCMR, Jan/Feb, 2003, p.14.

공급지에서 이루어지는 예방프로그램과 사전선별작업을 개선함으로써 위험도가 높고 의심이 가는 소수의 선적 화물에 검사작업을 집중시키면 검사작업의 효과를 높일 수 있다. 정부에서 주도하는 일부 보안조치들로 C-TPAT와 CSI 프로그램 등이 있다.

최근에 미국은 수입화물검사 효과성을 높이기 위해 타국 정부와 협력을 강화하고 있다. 이러한 일환으로 시행되고 있는 것이 CSI 프로그램이다. 이 프로그램은 선별 및 검사작업을 화물이 발생하는 선적항에서 수행하는 것으로 하자발생의 근본원인을 찾아내어 품질을 개선하고자 하는 전사적 품질관리기법과 그 맥을 같이 한다. CSI 프로그램은 선적항에서 선별, 검사작업의 일부를 수행함으로써, 테러사고의 위험을 감소시키며, 안정적인 화물의 흐름과 예측가능성을 보장해준다.

또한 최근 미국세관에서 채용한 자동표적시스템(ATS: Automated Targeting System)은 사전선적정보와 송하인 및 유사선적화물에 대한 과거 이력정보를 바탕으로 수많은 수입화물들을 선별하는데 사용되고 있다. ATS 기술은 선적화물의 급증이나 새로운 공급원으로의 단순한 이동, 운송경로의 변화 등 변동사항을 탐색한다. 대부분의 사전심사 및 검사대상 후보자들은 이러한 결과를 토대로 선정된다. 이와 함께 ATS를 통한 사전심사를 개선하기 위한 조치로 24hour rule을 시행중이다. 이에 따라 선적화물의 상세한 정보가 선적되기 24시간 전에 미국세관에 전자적으로 제공되지 않는 경우에는 컨테이너의 유입을 금지하고 과징금이 부과된다. 이 규칙은 ATS를 통한 선별검사의 창구를 제공할 뿐 아니라 수상한 컨테이너에 대해서 선적 전 검사를 실시할 수 있도록 기회를 제공한다.[57]

C-TPAT 프로그램은 공급사슬상 모든 당사자들이 전체 공급사슬의 무결성을 보장하기 위한 정책, 계획 및 절차들을 실행하도록 함으로써 운송과정에서 화물의

57) 양정호, 전게서, 2008.

변조위험을 낮추고, 광범위한 모니터링을 통해 불법거래를 방지하도록 하는 등 보안사고의 예방활동에 중점을 두고 있다.[58] 이는 자율규제(voluntary) 프로그램으로 항만 및 국경이동과정에서 신속한 통관절차를 보장해 주는 등 참여기업들에게는 다양한 인센티브가 주어진다.

그리고 2002년 10월에 착수한 SST(Smart and Secure Tradelane)는 미국의 항구에 입항하는 컨테이너를 대상으로 운송중인 컨테이너의 잠재적 변조를 식별하여 격리시키는 것을 목적으로 한다. 이러한 효과적인 절차통제는 최종검사과정의 지연을 방지하고 화물의 신속한 흐름을 보장할 수 있다.

제2절 해운기업의 보안사고에 대한 효과적인 대응전략

1. 위험관리전략[59]

해적과 테러공격에 의한 해상보안사고는 해상운송이 발생한 이후에 지속적으로 증가하고 있다. 예측하기 힘든 인명손실, 재산피해 등 막대한 영향력을 지녔다는 점에서 해상보안관리를 위한 위험평가 분석모델 개발이 필요하다.

9.11 테러사태를 계기로 기존에 화물도난, 마약과 같은 불법화물의 밀거래, 불법이민을 줄이는데 치중하였던 물류보안에 대한 인식이 변화하고 있다. 정부 및 기업들은 공급사슬 전반에 걸친 보안확보의 필요성을 인식하고 공급사슬의 효율성과 효과성을 지속적으로 유지하기 위한 다양한 방법들을 모색하고 있다.

테러위협으로 인한 불확실성의 증가는 산업의 글로벌화, 제품의 다양화, 제품수

58) 양정호, 상게서, 2008.

59) 양정호, 상게서, 내용 참조하여 재정리

명주기의 단축 등 비즈니스 환경의 변화로 인해 기업들이 이미 경험했던 문제들과 크게 다를 바가 없기 때문에 공급사슬의 성과를 높이기 위해 기업들이 이미 추진했던 공급사슬관리전략이나 위험관리시스템을 더욱 확고히 함으로써 보안효과를 높일 수 있다. 기업들은 테러위협을 차단하기 위해 공급사슬 파트너 및 정부당국과 긴밀한 협조체제를 구축하는 한편, 공급사슬의 가시성을 개선하고, 복원성을 높임으로써 테러공격으로 인한 물류시스템의 혼란에 대비하여야 한다.

1) 광범위한 추적 및 모니터링(Comprehensive Tracking and monitoring)

보안사고는 공급사슬상의 구조적인 결함으로 발생하는 경우가 많으며 어느 시점에 갑작스레 발생할 수도 있고 점진적으로 발생할 수도 있다. 어느 경우든 사고는 의외의 경우이거나 예상치 못한 경우가 대부분이다. 복잡하게 얽혀있는 글로벌 공급사슬 시스템의 구조상 위기의 징후를 탐지하기가 쉽지 않고, 설사 탐지가 가능한 경우라 하더라도 그 상황을 제대로 파악하기가 어렵다. 기업들은 대부분 위험의 징후를 인지하지 못한 채 사고를 방치함으로써 위기에 적절히 대응할 수 있는 시기를 놓치게 되고 위기에 직면하게 됨으로써 손실은 더욱 증가하게 된다.[60] 따라서 보안사고에 효과적인 대응하기 위해서는 보안사고 발생시 이를 즉시 탐지할 수 있는 능력이 요구된다. 통제할 수 없는 문제들은 신속하게 탐지되어야 하며, 문제의 정확한 소재 및 본질을 파악하여야 한다. 기업들은 공급사슬보안을 위해 선적화물, 재사용이 가능한 포장용구 및 운송수단에 대한 효율적이고 효과적인 모니터링 시스템을 도입하여야 한다. 또한 추적시스템은 여러 모순되는 사항들 중 우선순위를 정하여 이를 바로잡기 위한 적절한 조치를 취할 수 있도록 지원할 수 있어야 한다. 현재 화물의 발생지에서 최종 목적지까지 지속적으로 모든 선적화물을 모니터링 할 수 있는 시스템은 없지만 공급사슬 이벤트관리나 공급사슬 성과관리와 같은 기술들이 도입되면서 잠재적 사고를 감지할 수 있는 실시간 가시성 및 모

60) Paul Barnes and Richard Oloruntoba op. cit., pp.526~527.

니터링 역량을 제공하고 문제발생시 관련 당사자와 의사결정자에게 그 사실을 알림으로써 적절한 조치를 취할 수 있도록 지원한다.[61] 가시성 및 모니터링 시스템은 의사결정자에게 보안사고로 영향을 받는 특정 영역에 대한 구체적이고 정확한 정보와 함께 당해 문제의 규모를 제공할 수 있어야 한다.

2) 공급사슬 가시성의 개선

공급사슬상에서 이루어지는 모든 활동에 대한 정확한 정보를 적시에 파악하고 이를 토대로 특정 사건이 공급사슬 전반에 미칠 영향을 예측할 수 있다면 기업은 조달·생산·물류 및 결제에 관한 보다 합리적이고 효과적인 의사결정을 통해 공급사슬 운영의 효율성을 높이는 한편, 사고발생의 징후를 미리 인지하고 문제점을 조기에 시정함으로써 보안사고로 인한 파장이 공급사슬 전반으로 확대되는 것을 방지함으로써 피해를 최소화할 수 있다. 반면, 가시성을 확보하지 못하면 기업의 전략적 목표에 적합한 공급사슬 계획의 수립 및 변화하는 공급사슬 상황에 대한 체계적인 대응이 어렵기 때문에 공급사슬 전반에 대한 가시성을 개선하는 일은 기업경영에 있어서 매우 중요한 요인이다.

가시성은 원자재의 조달에서 최종소비자에게 완제품의 인도에 이르기까지 공급사슬 프로세스 전반에 걸친 물자의 이동, 거래 및 사건의 발생을 감지하고 통제할 수 있는 능력을 의미한다.[62]

가시성은 공급사슬 내에서 실시간으로 발생하는 정보에 대한 모니터링을 통해 공급사슬 프로세스 전반에 대한 완전한 시야를 확보하고 공급사슬 프로세스상의 문제를 미리 감지하여 공급사슬상의 변동에 선제적으로 대응함으로써 공급사슬 전

61) Hau L. Lee and Michael Wolfe, op. cit., p.17.

62) William Atkinson, “Gaining Supply Chain Visibility”, *SCMR*, Vol. 5. Issue 6, Special Supplement, November, 2001, p.4.

반에 미치는 효과를 최소화 하는데 그 목적을 두고 있다.[63]

공급사슬 전반에 대한 가시성은 공급사슬상 물자의 이동경로 및 위치, 재고수준, 도착예정시간 등 적시의 정확한 정보를 바탕으로 재고수준의 감소, 리드타임의 변동발생률 감소, 생산성 향상, 품절발생률 감소, 도난방지, 수입자와 고객, 그리고 공급자와의 관계를 개선하는데 도움을 준다.[64] 기업이 공급자, 생산자, 운송서비스 제공자와 함께 공급사슬상 재고의 소재 및 형태(원자재, 부품, 재공품, 운송재고 및 완제품)에 대해 명확히 파악하고 있다면 공급사슬상 일정 영역에서 보안사고가 발생한 경우 즉각적인 운송루트의 변경, 생산계획의 수정, 생산자원의 재배치 및 생산능력의 조정 등 적절한 대응을 통해 공급부족으로 인한 공장가동 중단이나 고객의 불만을 최소화할 수 있도록 지원한다. 송하인은 선적화물에 다한 가시성을 확보함으로써 운송화물의 이동상태를 파악하여 선적지연, 배송착오, 손상 등의 문제가 발생할 경우 적절한 조치를 취할 수 있다. 뿐만 아니라 예측의 정확성을 높이고 공급사슬이 순조롭게 운영되도록 함으로써 재고비용 및 급송비용을 절감하는 한편 예외적인 상황의 발생가능성을 줄임으로써 관리비용을 절감할 수 있다.

정보의 가시성을 확보하기 위해서는 적어도 두 가지 요건이 필요하다. 하나는 사건중심(event driven)의 공급사슬 운영에 관한 정보이고 다른 하나는 공급자, 제조업자, 물류서비스 제공자, 고객으로부터 적시의 정확한 정보를 확보하기 위한 정보시스템의 통합이다.[65]

---

63) Yossi Sheffi, “Supply Chain Management under the Threat of International Terrorism”, IJLM, Vol. 12, No. 2, 2001, pp.4~6.

64) Yossi Sheffi and James B. Rice, “A Supply Chain View of the Resilient Enterprise”, Sloan Management Review, Fall 2005, p.47.

65) Hau L. Lee and Michael Wolfe, op. cit., p.14.

3) 공급사슬의 유연성 및 복원성 확보

견고하고 복원력 있는(robust and resilient) 공급사슬 구조는 보안사고 발생시 공급사슬상의 혼란을 피하고 그 영향을 최소화하는데 도움을 준다. 견고한 공급사슬은 보안사고에 대한 취약성을 낮추고 복원성은 우발적인 사건이나 재난으로 불안정해진 시스템이 그 이전의 정상적인 상태로 복귀할 수 있는 능력으로[66] 공급사슬상 혼란이 발생하더라도 정상적인 상태로 신속하게 복귀할 수 있도록 해준다.

복원성을 확보하기 위해서는 만약의 사태에 대비하여 기업의 생산능력 비축, 재고수준의 증가, 공급선 다변화 등 공급사슬상 낭비적인 요소를 어느 정도 용인하여야 하는 바, 이로 인해 공급사슬의 효율성이 떨어질 수 있다. 하지만, 보안위험에 대한 공급사슬의 취약성을 낮추고 공급사슬 구조를 유연하게 함으로써 수시로 변하는 시장상황에 보다 신속하고 효과적으로 대응할 수 게 된다.[67]

견고한 공급사슬은 공급사슬이 정상적으로 운영되는 상황에서는 비용절감, 고객만족 및 고객관계를 향상시키는 한편, 공급사슬 혼란이 발생하는 동안에도 공급사슬의 정상적인 운영을 지속할 수 있는 구조를 말한다. Tang(2006)[68]은 공급사슬구조를 견고히 하고 복원성을 높이기 위해 공급자 다변화, 전략적인 재고유지, 운송방식의 다양화, 그리고 모듈화 및 지연전략을 통한 제품의 다양성 확보 등의 전략이 필요하다고 하고 있다.

---

66) Cranfield School of Management, Creating Resilient Supply Chains: A Practical Guide, report on behalf of the Department for Transport, 2003.

67) Ravi Sarathy op. cit., pp.45~47.

68) Christopher S. Tang, “Robust strategies for mitigating supply chain disruptions”, *International Journal of Logistics*, 9(1), March, 2006, pp.33~45.

4) 유연한 소싱 전략

1980년대 이후 많은 기업들은 장기적인 관점에서 공급자와의 관계를 보다 확고히 하고 복잡한 공급자관계를 관리하는데 소요되는 비용을 절감하기 위해 공급자의 수를 축소함으로써 공급네트워크를 단순화하고 있다. 이러한 전략은 조달 및 생산비용을 절감할 수 있는 장점이 있지만 테러위협의 증가와 보안사고로 인한 공급사슬의 중단 등을 고려할 때 이러한 전략의 수정이 불가피하다. 따라서 기업들은 공급자 다변화, 역내공급자의 활용을 통해 보안사고로 인한 공급사슬 혼란 및 시장의 수요변화에 유연하고 신속하게 대응하도록 하는 한편 기존의 전략을 유지하면서 공급네트워크를 이원적으로 활용함으로써 공급사슬의 효율을 지속적으로 유지할 수 있다. 가령, Dell은 컴퓨터 프로세서와 메인보드의 경우 Intel, 그리고 운영시스템의 경우 Microsoft와 강력한 단일공급자관계를 구축하고 디스크 드라이브와 같은 기타 부품에 대해서는 다양한 공급업자를 활용하고 있으며, HP는 조달비용을 절감하기 위해 수요가 안정적인 대부분의 프린터를 싱가포르에서 생산하는 동시에 북미시장에 신속하게 대응하기 위해 캐나다 밴쿠버에 추가적인 생산설비를 갖추고 있다.[69]

5) 제품 및 프로세스의 재설계

제조공정 및 제품 디자인에 있어서 규격화된 모듈을 사용하는 기업은 원자재 공급부족이나 조달상의 어려움에 유연하게 적응할 수 있으며, 시장에서 제품의 가용성에 심각한 영향을 초래함이 없이 우발적인 상황에 신속하게 대응할 수 있다. 또한 일부 제조업체들은 생산품목 및 선택사항의 수를 줄임으로써 수요예측의 어려움을 극복하고 있다. 선택사항의 축소는 위험의 분담을 보다 수월하게 하고 가변성을 낮추어 예측을 개선하고 전반적인 비용을 줄일 수 있다. Intel Systems Group은 2000여 종의 레지스터, 축전지, 다이오드 등을 35종으로 축소하여 비용을

69) Yossi Sheffi, op. cit., pp.2~3.

절감하는 한편 조달절차를 간소화함으로써 수요변화 및 공급난에 유연하게 대처할 수 있는 능력을 가지게 되었다.[70] 생산프로세스의 표준화 역시 기업들의 생산능력을 점차 공동화시켜 특정지역에서 공급중단이 발생하는 경우 다른 지역의 공급자를 활용할 수 있다.

제품의 최종형태를 마지막 순간까지 보류하는 지연전략(postponement strategy)은 보안사건이 발생하여 특정 부품의 공급부족이 발생한 경우 최종형태를 변경하여 수요를 충족시킬 수 있다. 주문생산(build-to-order) 시스템은 공급잉여지역의 부품 및 반제품을 급격한 수요증가나 공급부족이 발생하는 지역으로 전용함으로써 수요와 공급의 불균형을 해소할 수 있다. 일례로 HP는 공통된 디자인과 부품을 사용하는 프린터를 세계 도처의 물류센터로 배송하되, 변압기와 전원공급장치, 사용자 매뉴얼 등은 각 지역별로 주문을 받아 고객의 요구조건에 맞게 변형하는 지연전략을 활용하였다. 이러한 방법을 통해 HP는 보편적인 프린터에 대한 총수요를 예측하고 지역별 특성 및 소비자의 요구가 다른 부품에 대해서는 개별적인 예측을 통해 재고비용을 줄이고 리드타임을 단축할 수 있었다.[71] 이렇듯 제품 및 프로세스의 재설계로 다양한 생산능력의 공유가 가능해지면서 생산의 유연성이 확보되고 수요의 급증이나 공급중단에 신속하고 유연하게 대응할 수 있다.

6) 효율적이고 효과적인 재고관리

기업들은 JIT 및 Lean[72] 생산체제를 통해 지속적으로 재고를 감축하기 위해 노

70) Yossi Sheffi, “Resilience Reduces Risk”, Logistics Quarterly, Vol.12, Issue 1, March 2006, p.13.

71) Yossi Sheffi, op. cit., pp.4~6.

72) Lean은 모든 공정상의 낭비(waste)를 제거하고 공급사슬 프로세스를 최적화하여 속도와 흐름을 증진하기 위한 활동으로 도요타 생산시스템(Toyota Production System)에 그 뿌리를 두고 있다(Thomas Goldsby and Robert Martichenko, Lean Six Sigma Logistics, J. Ross, 2005, p.4).

력해 왔다. 하지만, 9.11 테러사태 이후 기업들은 이러한 시스템 하에서 보안사고나 예상치 못한 사건이 발생시 공급프로세스가 쉽게 혼란을 겪을 수 있다는 점에서 문제를 제기하기 시작하였다. 일부 기업들은 JIT 생산방식이 지니는 많은 이점에도 불구하고 보안사고로 인해 운송시스템에 혼란이 야기될 경우에 대비하기 위하여 부품을 대량으로 주문하고 안전재고를 늘리고 있다.

일정한 서비스 수준을 유지하기 위해 안전재고를 일정수준으로 유지하는 것은 공급사슬상 리드타임의 변동에 대비하기 위한 것이다. 따라서 평균 리드타임을 줄이는 것 보다는 리드타임의 변동을 줄이는 것이 안전재고를 감축하는데 도움이 된다. 공급사슬의 불안정에 대비하기 위해 JIT 전략을 재검토할 필요가 있지만, 그렇다고 재고보유량을 늘리게 되면 그에 따른 비용도 만만치 않다.

따라서 기업들은 적정수준의 재고를 유지하기 위해 품절위험과 재고관리비용 간의 상충관계를 평가하기 위한 과학적인 재고관리기법을 도입하여야 한다. 이를 위해 보안사건과 관련한 공급중단의 위험을 파악할 필요가 있다. 하지만, 대부분의 전통적 재고관리시스템은 수요의 불확실성만을 다루고 있다.

그리고 기업들은 수요와 공급의 불확실성을 모두 커버할 수 있는 재고관리시스템을 개발할 필요가 있다. 이를 위해 재고를 이원적으로 관리할 필요가 있다.[73] 즉, 기업경영상 발생하는 예측상의 오류와 시장 환경의 변화에 대응하기 위해 일정 수준의 안전재고를 비축하는 한편, 테러위협 등 보안사고로 인한 공급사슬의 혼란에 대비하기 위해 전략적으로 비상재고(emergency stock)를 지정하여 이는 일상적으로 발생하는 수요변동에 사용하지 않고 공급사슬 혼란이 발생하는 최악의 경우에만 사용도록 하는 것이다. 전략적으로 유지되는 비상재고는 일상적인 수요예측에 관계없이 재고가 소진되는 즉시 보충되도록 관리하여야 한다. 이는 미국이

73) Yossi Sheffi, op. cit., pp.3~4.

오일파동에 대비하여 전략적으로 오일을 비축하는 것과 유사하다.

기업들은 예측실패로 인한 위험을 분산하기 위해 재고를 집중시켜 관리하되, 보안상 일정 지역에 테러공격이 자행되는 경우 그로 인한 손해를 완화하기 위해 기업의 자산 및 인력을 분산시킬 필요가 있다. 또한 분산 배치된 재고를 중앙에서 통합하여 관리함으로써 재고관리비용을 절감하는 한편, 재고의 편중과과부족을 해소할 수 있다.[74]

7) 공급사슬 파트너 간 신뢰구축 및 협업

공급사슬에는 기업을 비롯하여 공급파트너, 정부기관, 그리고 유통업자 및 중개업자 등 많은 당사자들이 참여하게 된다. 복잡한 공급사슬 구조상 보안위험은 대부분 가장 취약한 연결지점에서 발생하기 때문에 공급사슬에 참여하는 모든 당사자들에게 보안에 대한 경계 및 주의가 요구된다. 기업들은 보안에 대한 부담을 덜기 위해 국제물류보안제도 및 기업의 보안요구사항을 준수하는 공급파트너를 선호하게 되고 안정적으로 물자를 조달할 수 있는 지역에 공급네트워크를 집중시킬 수 있다. 즉, 공급사슬 보안을 위한 공급네트워크의 구성에 있어서는 비용보다 공급사슬 당사자 간의 신뢰가 중요한 요소가 된다.

이와 함께 기업들이 보안을 강화하고 보안관련 솔루션, 투자, 기술, 정보, 실행 및 혜택을 공유하기 위해서는 공급사슬 전반에 걸친 협력이 필요하다. 기업들은 공급사슬보안의 관리 및 통제를 위한 프로세스와 규칙을 개발하고 당사자들에게 보안을 위한 일정한 역할과 책임을 할당하는 한편, 물류보안규정의 준수를 보장하도록 하는 등 공급사슬 파트너와 협력할 필요가 있다.[75]

---

74) Hau L. Lee and Michael Wolfe, op. cit., p.14.

75) Ravi Sarathy op. cit., p.47.

이와 더불어 국경을 초월하여 이루어지는 글로벌 공급사슬활동의 특성상 기업은 지역 및 연방정부와 협력하여 효율적이고 효과적인 보안시스템의 달성을 위해 노력하여야 한다.[76] 정부는 주로 국경 및 보안설비 강화에 주력하고, 민간 기업들은 화물보안, 공급사슬 파트너와의 협력, 그리고 인력에 대한 보안교육 및 훈련에 주력하는 것이 바람직하다. 공급사슬상의 보안을 개선하기 위한 민관 협력프로그램은 공급사슬상의 취약부분을 발견하고 공급사슬 프로세스를 합리화하는데 도움이 되며, 공급사슬 당사자 간 의사소통을 촉진시키고 정부 및 참여기업이 핵심정보를 공유할 수 있도록 한다.[77] C-TPAT와 더불어 SST 및 OSC와 같은 공급사슬 보안을 위한 민관협력프로그램은 보다 시의적절하고, 정확하고 완전한 정보접근을 통해 기존의 비즈니스 프로세스를 단순화하고 보다 합리적인 의사결정을 도와줌으로써 상당한 재정적 효과를 볼 수 있다고 한다.[78]

8) 공급사슬 보안 개선을 위한 조직구조 개편

공급사슬보안의 개선을 위해 기업은 보안시스템의 개발 및 실행과 관련하여 집중화와 분권화를 균형 있게 추진하여야 한다. 정보공유를 통한 조직 구성원들 간의 원활한 의사소통과 의사결정권한의 이양은 핵심 당사자들이 공급사슬 프로세스상의 문제를 사전에 감지하고 적절한 조치를 취할 수 있도록 함으로써 보안사건에 신속하고 유연하게 대응할 수 있도록 한다.

이를 위해 기업은 보안책임을 담당할 최고보안담당 책임자(Chief Security Officer)를 지정하여 기업의 전략적 목표와 보안활동 간의 불균형을 시정하고 다양

76) Yossi Sheffi op. cit., pp.6~9.

77) David J. Closs & Edmund F Mc Garrell, Enhancing Security throughout the Supply Chain, IBM Center for The Business of Government, April 2004, p.37.

78) Smart&Secure Tradelanes, Phase One Report, November 2003.

한 보안계획들을 조정·검증함으로써 테러공격 이후에도 기업 활동이 지속될 수 있도록 보장하는 한편, 교육 및 훈련을 통해 기업 구성원들의 보안의식을 높이고 보안에 대한 인식이 조직 전체로 확산될 수 있도록 분위기를 조성하여야 한다.

이와 함께 기업들은 보안사고로 시스템이 와해되는 경우에 대비하여 재고 및 공급처, 그리고 업무지식 및 비즈니스 프로세스에 대한 백업시스템을 구축할 필요가 있다.[79] 직원들의 업무지식은 대부분의 기업들에게 매우 중요한 자원이라 할 수 있다. 만약의 사태에 대비하여 잉여인력을 유지하기는 것은 어렵기 때문에 주요 업무프로세스를 문서화하여 언제라도 이용할 수 있도록 하여야 하며, 가능하다면 인력의 교차 훈련을 통해 부서 간 전용이 가능하도록 하여야 한다.[80] 이와 더불어 기업전반의 비즈니스 프로세스와 업무관행을 표준화함으로써 업무의 적응성과 정확성을 높일 수 있으며, 보안사고 발생으로 공급사슬의 운영상 차질이 발생하더라도 인력 및 프로세스를 유연하게 전용할 수 있다.

2. 공급사슬 보안기술의 활용[81]

최근 컨테이너 보안, RFID 테그의 활용, 컨테이너 적격심사와 같은 보안기술이 점차 안정되어 가고 있다. 새로운 보안기술의 활용은 공급사슬 당사자의 식별 및 공급사슬 결절점에 대한 접근통제, 컨테이너의 안전한 적재 및 전자적하 목록(electronic manifests)을 통한 검증, 컨테이너 내용물의 변조를 방지하는 봉인장치, 소프트웨어를 활용한 우범화물의 자동선별, 컨테이너화물의 적재과정을 추적하고 이동을 감시하는 GPS(Global Positioning System) 및 RFID 기술 등 여러 방면에

79) Yossi Sheffi op. cit., p.4.

80) 세계무역센터에서 7000명의 직원을 거느리고 금융서비스를 제공하는 Solomon Smith Barney는 한순간에 이들을 모두 잃었다. 하지만 이 기업은 뉴저지에 있는 백업사이트와 일련의 백업프로 세스를 가동하여 12시간 만에 다시 업무를 재개할 수 있었다.

81) Ravi Sarathy op. cit., pp.47~48.

서 공급사슬 보안시스템을 강화하는데 중요한 역할을 한다. RFID를 비롯하여 바코드, 전자봉인장치(electronic seal), GPS, 무선통신네트워크 등의 물류보안기술은 공급사슬 시스템과 연계하여 정보를 수집하고, 수집된 정보를 변환·분석하여 적절한 당사자에게 제공함으로써 선적화물의 무결성을 보장하고 운송 중 변조가능성을 낮추는 한편, 공급사슬의 가시성을 개선할 수 있다.

특히 RFID 기술은 자동침입탐지, 방사능 등 위험물질의 검색, 컨테이너의 위치 및 상태에 대한 실시간 무선송신을 통해 공급사슬 보안을 강화하는데 도움을 준다.51) 미국 국토보안국(DHS: Department of Homeland Security)에 따르면 능동형 RFID(active RFID)를 장착한 컨테이너는 도착지에서 검사가 생략되고 즉시 통관 대상이 된다고 한다. 이와 같은 조치는 운송시간의 단축과 재고수준의 감소효과가 있을 뿐 아니라 컨테이너의 보안상태나 내용물에 대한 검증이 용이해 통관절차가 신속히 이루어짐에 따라 위급상황에서도 공급사슬의 효율성을 지속할 수 있다는 점에서 많은 혜택을 제공한다.52) 하지만 이러한 보안기술은 보안을 향상시키기 위한 유일한 방법도, 오류가 없는 절대 안전한 방법도 아니다. 보안기술은 전반적인 공급사슬의 재설계와 전체 공급사슬 및 업계, 정부 및 국제기구와의 협업을 통해 보완되어져야 한다.

다양한 사이버 위험에 노출되어 있는 해운산업의 해상 사이버 보안 대응을 위해 미국과 캐나다는 선박의 보안과 항만 및 해운산업에 대한 자발적 가이드라인 개발에 대한 필요성을 IMO 해사안전위원회(MSC, maritime safety committee) 94차 회의에 제기하였다.[82)]

MSC 95차 회의에서는 사이버 보안의 범위가 해양산업전체가 아닌 선박에 대한 사이버 보안 지침을 개발하는 것으로 결정되었으며, 발트국제해사협의회(BIMCO;

82) 강남선, “선박 사이버 보안에 대한 기술적 분석”, 「한국마린엔지니어링학회지」, 42(6), 2018, pp.463-471.

baltic and international maritime council), 국제건화물선주협회(INTERCARGO, international association of dry cargo shipowner), 국제해운회의소(ICS; international chamber of shipping), 국제유조선주협회(INTERTANKO; international association of independent tanker owner), 국제정유사포럼(OCIMF; the oil companies international marine forum) 등에서 제안된 선박사이버 보안 가이드라인(the guidelines on cyber security onboard ships)이 제시되었다.

IMO는 MSC 96차 회의에서 해상 사이버리스크 관리에 대한 임시지침(MSC.1/Circ. 1526)을 승인하고 MSC 98차 회의에서 회람서를 승인하였으며, 기국들에게 안전관리시스템에 사이버리스크 관리를 포함하도록 권고하기로 합의하였다[13][14]. 이에 따라 ISM 적용 선박은 2021년 1월 1일 이후 사업장의 안전관리적합증서(DoC; document of compliance)의 첫 번째 연차 검사일까지 DoC에 사이버리스크 관리가 포함되도록 권고되고 있다.

OCIMF는 TMSA(the tanker management and self assessment)의 효율화 작업의 일환으로 사이버보안을 포함한 항목을 추가하여 TMSA3을 제정하였으며, RIGHTSHIP에서는 사이버보안을 포함한 추가 검사 사항을 반영하여 RIGHTSHIP 검사표를 최신화하였다[9]. 또한 ISO/TC80/SC 1에서는 해상에서의 사이버 보안을 위해 해운선사 안전 관리 시스템으로서의 사이버 안전 관리 시스템을 수립, 구현, 유지 및 지속적인 개선을 위한 지침 제정 작업이 이루어지고 있다[16].

1) BIMCO[83]

BIMCO 선박 사이버 보안 가이드라인에서는 사이버 보안을 위험 요소 식별, 식별된 위험에 대한 취약점과 위험 노출 평가, 평가 결과에 대한 보호 방안, 비상 대

83) 강남선, 상게서, 2018, pp.463-471 내용 재정리.

책 수립, 비상대책에 따른 대응으로 정의하고, 가이드라인의 적용을 받는 선박에 탑재된 잠재적 취약장비를 규정하였다.

사이버 공격은 피싱, 워터홀링 등 일반적인 기술을 사용하여 불특정 다수의 선사 및 선박의 시스템 과 데이터를 공격하는 무차별 공격과 특정 정보를 캐내기 위한 스피어싱(spear-phishing), 대규모 네트워크 공격을 위한 봇네트 배포(deploying botnets) 등의 방법을 이용하여 선사 및 선박의 특정 시스템 또는 데이터를 공격하는 표적 공격으로 구분한다.

사이버 공격은 조사/정찰(survey/reconnaissance), 전달(delivery), 파괴(breach), 영향(affect)의 4단계로 구분된다. 조사단계에서는 사이버 공격을 위한 방법 수집과 개발, 전달 단계에서는 공격 도구의 배포, 파괴 단계에서는 실질적으로 시스템과 데이터에 대한 공격이 이루어지며, 영향 단계에서는 공격으로 인한 피해가 발생된다.

사이버 보안에 대한 취약점은 선사 또는 선박의 IT(information technology), OT(operation technology) 및 정보와 데이터 적용 현황에 따라 달라지며, 위험 노출도 평가는 CIA (confidentiality, integrity and availability) 모델 프레임워크에 따라 다음의 항목에 대한 3단계 영향을 평가한다.

첫째, 선원, 승무원, 화물 및 승객에 대한 정보나 데이터에 대한 접근
둘째, 사이버 공격으로 선박의 안전 및 운항 효율 관련 자료의 무결성 상실
셋째, 정보 또는 데이터 변조 및 서비스 중단으로 인한 데이터 가용성 상실

선박 사이버 보안 가이드라인에서는 사이버 보안에 대한 대응방안을 선박 보안 담당자나 IT 부서장이 아닌 경영자선에서 정의될 것을 권고하고 있으며 사이버 보안 위험에 대한 대응 방안으로 기술적인 방안과 절차적인 방안을 제시하였다.

2) 영국선급

영국선급(LR, lloyd's register)은 해운산업분야의 사이버 보안을 다룬 CES(cyber-enabled ship) 가이드라인을 발표하였다. CES 가이드라인은 사이버 시스템 정의, 6가지 위험 영역에 대한 고려사항, CES에 대한 평가방법으로 구성된다. CES 대상 범위는 항해, 기관장비 뿐 아니라 선박에 설치된 센서, 모니터링 시스템, 컨트롤 시스템, 하드웨어와 같은 ICT 장비, 해사데이터, 빅데이터, 위성 및 라디오 통신, VoIP, E-mail 등이 포함된다. CES 가이드라인은 주요 위험영역을 일반적인 시스템과 5가지 경계로 구분하고 이에 대한 고려사항을 제시하였다.

첫째, 시스템은 산업표준에 따라 구현, 관리되어야 하며 위험기반 접근법에 따라 안정적인 운영과 시스템 복구 기능을 보증해야 한다. 시스템 구현 및 관리에 대한 산업 표준은 ISO/IEC/IEEE 15288(system and software engineering - system life cycle process)와 ISO/IEC/IEEE 12207(system and software engineering - software life cycle process)이며, 위험기반접근법은 영국 선급의 ARBD (assessment of risk based design) 기법, NIST(national institute of standards and technology) 표준, SP800-64(security considerations in the system development life cycle)를 적용할 수 있다.

둘째 휴먼시스템(human-system)은 의존성과 신뢰성을 확보하기 위하여, 시스템 개발 및 운영에 대한 구조화된 HCD(human centred design) 접근이 필요하다.

ICT 기술은 선박의 안전과 운항, 육상 지원업무 등 전통적인 작업을 지원하거나 일부 대체할 수 있으므로 각 장비의 개별적인 사용자 인터페이스가 아닌 선원과 육상직원 모두 안전하고 효율적으로 작업이 가능한 통합 사용자 인터페이스가 필요하다. 통합 사용자 인터페이스 개발은 ISO 9241-210(human centred design for interactive systems)에 따라 휴먼시스템 개발 및 운영에 대한 구조화된 HCD 접

근이 필요하다.

셋째, 네트워크 및 통신은 해상표준을 준수해야하며, 우선순위에 따른 통신과 데이터 무결성을 보장해야 한다. 선박 네트워크 및 통신은 해상환경에 적합한 표준을 만족하고 중요한 통신 인프라에 대한 스페어를 확보해야하며, 설치된 시스템에 대한 적절한 유지보수 절차가 필요하다. 뿐만 아니라 비상상황에서 안전 또는 경영 시스템이 우선시 될 수 있도록 사용 가능한 통신 대역폭에 접근할 수 있는 접근성과 편의성을 확보해야 한다.

넷째, 소프트웨어는 국가 표준이나 IEC 61508과 같은 국제 표준을 만족해야하며, ISO 9001 표준에 적합한 생산, 유지보수 등을 보장해야한다.

다섯째, 데이터 신뢰성을 위하여 시스템 설계 단계에서 무결성(integrity), 유효성(availability), 인증(authentication), 비밀(confidentiality), 허가(authorization), 부인방지(non-repudiation)를 고려해야한다.

여섯째, 사이버 보안은 시스템 개발에 미치는 영향뿐 아니라 직원의 교육, 조직문화 등의 사항을 고려해야한다. LR은 진화되는 새로운 기술을 신속하게 채택할 수 있도록 CES 가이드라인에 Figure 3의 프로세스에 따라 특정 시스템을 평가할 수 있는 통합된 위험 기반 접근 방식을 적용한다.

3) 미국선급

미국선급(ABS, american bureau of shipping)은 ABS Cyber Safety TM 시리즈의 일부로서 시스템, 선박 및 플랫폼에 대한 사이버 보안 가이드라인(the application of cyber security principles to marine and offshore operations) VOLUME 1 : CYBER SECURITY를 발표하였다.

ABS 사이버시큐리티는 모범 사례(best practice)를 통해 선박 및 플랫폼에 대한 사이버 보안 가이드라인을 제시하였다. best practice 구조는 기본 기능 (basic capability), 개발 기능 (developed capability)으로 구성되며, 사례, 프로그램 및 프로세스, 리스크 이해 및 관리, 보호된 리소스 및 접근으로 구분된다.

기본 기능은 9가지 기능으로 비즈니스 또는 운영 체제를 지원하기 위해 주로 사용되는 정보 기술 기반의 기능이다. 기본 기능은 반드시 조직 내에서 개발, 구현되어야 하며 명확하게 문서화되고, 사용되고, 지원되고, 유지되어야 한다. 개발 기능은 사이버 보안의 기본 기능을 보다 개발적 기능으로 확장하는 방법을 다루며 데이터 보호, 성능 시스템과 보안 시스템의 모니터링, 사고 시 복구 기능 어플리케이션 패치 등에 대한 best practice를 제시하였다. ABS 사이버 시큐리티는 기본 기능, 개발 기능에 대한 best practice외에 엔지니어링 제공, 설계 관리 도구, 투자 통제 실시와 같은 부가 기능에 대한 best practice도 제시하였다.

4) OCIMF TMSA & RIGHTSHIP

OCIMF는 유조선 선박 운영자가 안전관리 시스템을 평가, 측정 및 개선하는데 도움이 되는 표준 프레임 워크를 제공하는 유조선 관리 및 자체평가 우수 사례 안내서인 TMSA 3차 개정판을 2017년 4월에 발표하였다. 개정된 TMSA 3에는 해상 보안을 다루는 element 13이 포함되어 있으며, 사이버 보안 관련 주요 요구사항은 Table 5와 같다. Inspection and assessment report for dry cargo ship 검사에서는 기존 선박 점검표(FOD06(10))에 Table 6의 사이버 보안을 추가한 검사 사항을 반영하여 RIGHTSHIP 점검표를 개정하고, 2017.05.11.부터 검사에 적용하고 있다.

산업계와 각 선급에서 발표되고 있는 사이버 보안 가이드라인에는 사이버 보안

에 대한 인식의 개선과 이행을 위한 내부 절차, 기술 및 교육이 언급되고 있다.

따라서 본 연구에서는 BIMCO에서 제안한 사이버 보안과 관련해서 보안이 강화된 네트워크 구성, 선내 통합 네트워크 관리, 데이터 보안, 선박용 안티바이러스 서비스로 구분하고 이에 대한 기술을 제안하고자 한다.

(1) 보안이 강화된 네트워크 구성

현재 선박에서는 네트워크의 운용, 설치 편의성을 위해 일부 게이트웨이와 스위치를 사용하여 구역별로 네트워크를 분리하고 업무용 PC와 개인용 PC에 외부 통신을 제한적으로 허용하고 있다. 최근 선박과 육상간 데이터 공유와 개인 통신에 대한 요구가 증가하고 있어 외부 통신에 대한 개방이 필요하지만 현재 선박에 설치된 일부 게이트웨이와 스위치만으로는 사이버 보안에 대한 대응이 어려워 보다 강화된 네트워크 구성이 필요하다. 대부분의 사이버 보안 사고는 사용자 또는 시스템이 권한 밖의 시스템 또는 데이터를 사용하여 발생되기 때문에 운영 목적에 따라 네트워크를 구성하고 접근 권한을 부여하며 VPN, 방화벽과 같은 보안 장비를 운영하여야 한다. MiTS(maritime information technology standard)에서 제안한 Figure 6의 선육간 네트워크 구성과 같이 주요 네트워크와 시스템을 식별하여 한 네트워크에서 사이버 사고가 발생되어도 다른 네트워크에 영향을 미치지 않도록 선내 네트워크를 구성하여야 한다.

구분된 네트워크에 시스템 접근 권한을 정의하고, 각 네트워크 영역과 노드 사이에 방화벽, 게이트웨이 등을 설치함으로서 외부의 사이버 공격에 대비할 수 있다. 특히 외부통신 구간에 VPN을 설치하면 VPN 장비의 인증을 거친 후 선내 시스템에 접속할 수 있으며, 네트워크 트래픽이 암호화되어 방화벽을 통한 서비스 통제, 접근 대상 서비스 인증을 거치므로 보다 높은 보안 수준을 가진 선내 네트워크를 구성할 수 있다.

(2) 통합 네크워크 관리

대부분의 사이버 보안 사고는 사용자 또는 시스템이 권한 밖의 시스템 또는 데이터를 사용하여 발생되기 때문에 선육간 통신 구간에 대한 모니터링을 통해 사이버 공격을 감지할 수 있지만 현재 선박에는 이러한 시스템이 부재하여 사이버 공격에 대한 신속한 대응이 어려운 상황이다. 위성포트를 모니터링하면 인가되지 않은 포트의 연결과 비정상적인 통신 패턴 및 권한 밖의 사용자 또는 시스템 접근을 실시간으로 확인하여 선육간 통신 구간에서의 사이버 공격/위험을 감지할 수 있다. 또한 선내에 설치된 방화벽, 게이트웨이, 무선 AP(access point)를 연동하여 외부 침입, 내부 위험 감지 등을 확인하며 위험감지 시 해당 네트워크 및 노드의 방화벽, 게이트웨이, AP를 제어함으로서 다른 네트워크로의 2차 피해를 방지할 수 있다.

2006년 해사노동협약의 발효(2013)로 인해 선박 환경 및 선원복지환경 개선요구가 증가하고 있으며, 스마트 기기의 대중화에 따른 인터넷기반 유무선 통합기술의 수요와 선원 개인 통신에 대란 요구가 꾸준히 증가하고 있다. 이에 따라 일부 대형 해운선사에서는 선원 거주공간에서의 개인 네트워크 환경을 제공하고 있다. 사이버 보안 사고의 원인은 인적과실, 특히 웹서비스를 이용하는 과정에서 발생되는 경우가 가장 많기 때문에 웹서비스 환경에서의 개인 통신환경에 대한 보안 기술이 필요하다. 현재 선박에서 사용되고 있는 웹서비스 제공 방법은 Figure 8과 같이 사용자가 파일, 연결, 웹 페이지 등과 같은 자원을 프록시 서버에 요청하면 프록시 서버는 웹사이트와 클라이언트사이에서 대신 통신을 수행하며, 원격에 요청된 자원을 캐시하여 자원 재 요청 시 프록시 서버 내 정보를 제공하고 있어 보안에 취약한 단점이 있다.

이러한 단점을 보완하기 위하여 프록시 서버를 육상시스템에 구성하여 IP, 사용자, 도메인 등에 대한 필터링 정책을 관리하고 사용자 계정을 생성하여 개인 통

신 환경을 관리하며, 해운선사에서 지정한 필터링 정책에 따라 웹사이트의 멀티미디어 데이터를 필터링하고 텍스트와 이미지를 압축함으로서 경제적이고 보안이 강화된 개인통신환경을 제공할 수 있다.

최근 선박 장비의 IT화, 네트워크화되면서 다양한 기능과 편의를 제공하는 반면, IT 기술의 고도화와 개별적으로 운영되는 장비수 증가로 인해 제한된 인원과 IT 전문지식이 부족하여 외부 공격에 대한 모니터링과 사고발생 시 신속한 대응이 어려운 단점이 있다. 선내 설치된 다양한 IP 장비의 운용, 설정과 MS 운영체계를 사용하는 선내 컴퓨터를 Figure 10과 같이 선내 각 네트워크 영역과 노드 사이에 설치된 방화벽, 게이트웨이와 각 네트워크에 설치된 IP 기반의 모든 장비, 컴퓨터를 SNMP(simple network management system)기반으로 모니터링하고 제어할 수 있다.

SNMP를 이용하여 TCP/IP 기반의 네트워크에서 정기적으로 네트워크상의 각 IP 장비에 대한 여러 가지 정보를 수집하여 IP 장비의 상태를 모니터링 할 수 있으며, IP 장비 또는 네트워크에 비인가장치의 연결을 실시간으로 확인하여 비인가 장비의 접속으로 발생되는 위험을 예방할 수 있다. 또한 IP 장비의 OS 버전, 보안상태 및 응용 프로그램의 버전을 확인하고 육상에서 최신의 업데이트 파일을 받아 업데이트가 필요한 IP 장비에 자동업데이트 함으로써 사람의 접근이 어려운 곳에 설시된 IP 장비도 OS, 보안 패치 등을 효율적으로 관리할 수 있다.

선내 수집 데이터를 활용하는 선박 및 육상 어플리케이션과 서비스가 증가하면서 선내 및 선육간 네트워크 통신 구간에서 데이터 보안의 중요성이 강조되고 있지만 선내, 선박과 육상간 데이터 통신 구간에서 해사데이터에 대한 보안이 부재하다. 선박과 육상간 데이터 통신구간에서 데이터 보안을 위해서는 해사데이터를 암호화하고 통신구간에 SSL(secure sockets layer)과 같은 보안 기술을 적용할 수

있다. SSL은 사이버 공간에서 전달되는 정보의 안전한 거래를 보장하기 위한 인터넷 통신규약 프로토콜으로, 해사 데이터에 SSL을 적용하여 서버와 클라이언트의 진위 확인, 암호화키와 관련된 협상, 상위 응용프로그램이 정보를 서버와 교환하기 전에 서버의 진위를 확인함으로서 해사 데이터의 보안을 확보할 수 있다.

대부분의 선박에는 보안 관련 소프트웨어가 설치되지 않고 OS 업데이트가 이루어지지 않고 있어 바이러스 감염에 쉽게 노출되어 있으며, 시스템 호환 등과 같은 문제가 발생되고 있다. 이러한 문제점은 발표된 여러 해상 사이버 보안 가이드라인에도 명시되어 있어 선박용 안티바이러스 기술의 적용이 반드시 필요하다.

해상통신환경은 육상과 달리 통신 사용량과 대역폭이 제한되기 때문에 육상에서와 같은 방법으로 바이러스 패치를 업데이트할 수 없다. 따라서 선박용 안티바이러스 서비스는 Figure 11과 같이 육상에서는 안티바이러스 제조사로부터 최신 업데이트 파일을 수신하여 기존 파일에서 추가된 최신의 패치 파일만 선별하여 선박으로 전송한다. 선박에서는 최신 업데이트 패치 파일을 수신하여 안티바이러스 제조사와 업데이트 패턴을 공유함으로써 경제적인 방법으로 선박에 안티바이러스 서비스를 제공할 수 있다.

제5장 결 론

국제 분업화와 제 삼국을 경유하는 국제 교역이 증가함에 따라 위해 물품과 불법 화물이 증가하고 있으며, 전 세계적으로 FTA에 따른 경제 가속화로 자유무역이 확대되고 국가 간 교역량이 증가됨에 따라 밀수품과 위해식품 등 불법적인 요소를 내재한 물품들로 인한 위험성이 증가하고 있다.

또한 국제무역 환경에 다양한 위해 요소로, 국제 물류 공급망에 영향력을 미치고 있는 국제 범죄 조직들의 활동으로 인하여 국제적 안전과 경제 질서에 혼란이 가중되고 있다. 2001년 발생한 미국 9·11테러 사건은 국제무역 보안에 대한 관심을 증대시켰다.

이에 따라 항공운송 및 해상운송의 단편적 운송수단 보안 관리에서 국제 물류 화물의 공급사슬 전 과정에 대한 보안 관리가 요구되고 있다. 보안관리 대상은 제조와 운송, 보관, 정보 영역 까지 확대되고, 보안을 강화하기 위한 추가적인 절차를 수행해야 함에 따라 국제무역의 효율성이 저하되고 있다.

그리고 새로운 교역장벽으로 인한 수출입 안전관리 제도의 시행 여부에 따라 혜택과 불이익이 명확하게 나타나고 있고, 수출입 안전관리 제도의 강화에 따라 관련 기술 개발과 국제 표준에 대한 글로벌 기업들 간의 경쟁이 치열해지고 있다.

미국의 테러사건 이후 해양산업과 상선에 대한 테러 경각심이 높아지고 있다. 자체의 방어 무기체제 없이 광활한 해상을 활동 무대로 하는 상선은 인명, 선박과 화물의 재산, 환경 및 경제에 미치는 직·간접 영향의 광대성 때문에 테러의 목표물이나 수단으로 사용될 개연성이 높다.

따라서 국가와 국가, 국가와 민간기업 간의 국제 물류 공급망 보안 강화를 위한

협력과 각국 세관 간의 협조 체제를 통해 활발한 정보 교환으로 고위험 화물을 식별하고 국제 물류 공급망의 조기 통제능력 향상 등 위험관리 전략을 구축하고 있다. 9·11 테러 피해 당사국인 미국은 테러 위협에 대응하고자 다각적인 방어 전략을 추진하였고 국토 안보부 설치 등 행정조직을 대폭 개편하고, 화물정보 24시간 전 신고제도, 9·11 테러대책 이행법, SAFE Port Act, CSI 도입 등 다양한 물류 보안 제도를 구축하였다. 또한 전 세계적으로 테러공격이 확대되면서 국제기구 및 세계 각국과 공조하여 글로벌 물류 보안체제 구축을 주도하고 있다.

본 연구에서는 선박보안사고의 현황과 원인을 파악하여 선박보안관리의 특성을 조사하고 선박보안관리시스템의 취약점을 분석하였다. 또한 해상공급사슬보안의 개념과 특징, 보안위험과 공급사슬의 취약성을 조사하였다.

국제기구의 해상공급사슬보안제도 및 주요국의 해상공급사슬보안 인증제도 현황을 분석하여 해상공급사슬보안의 문제점을 개선하고, 모든 물류 구역에서 발생할 수 있는 테러 공격과 같은 보안 사고를 예방함으로써 해상공급사슬이 실시간으로 원활히 운영되도록 유도하였다. 또한, 해운회사의 해상공급사슬보안 요소 및 범위를 확립하고, 보안위험을 예방하고 위험성을 감소하기 위하여 수립된 대책 등 관련 선행연구를 검토하였다. 이를 통해 유형별 해상보안위험에 효과적으로 대처할 수 있는 보안체계 구축 방법과 해운회사의 해상공급사슬 보안사고 예방을 위한 효과적인 리스크 관리전략을 제안하였다.

향후에는 해양에서 보안취약성을 보완하고 보안위험을 낮추기 위해 선박의 특성을 고려한 보안 시스템 및 보안장비의 개발에 관한 연구가 지속적으로 수행되어야 할 것이다. 특히 항만, 연안, 영해에서 선박의 보안수준을 높이고 체계적인 대응을 위한 보안지원세력의 일원화와 체계적인 해안 보안 시스템의 구축에 국가적인 노력이 필요하다.

참고 문헌

<국내 문헌>

강남선, “선박 사이버 보안에 대한 기술적 분석”, 「한국마린엔지니어링학회지」, 42(6), 2018, pp.463-471.

고현정, “국제물류보안 인증제도 동향 및 시사점에 관한 연구”, 「한국항만경제학회지」, 27(2), 2011, pp.333-354.

고현정, “우리나라 물류보안 인증제도 효율화 방안에 관한 연구”, 「로지스틱스연구」, 19(2), 2011, pp.65-85.

김수엽, “항만물류보안산업의 발전방안 연구”, 한국해양수산개발원, 2009

김영균, “항만터미널의 유형과 공급사슬보안경영 활동이 경영성과에 미치는 영향에 관한 연구”, 한국해양대학교 박사학위논문, 2011.

김태운, “한국 해운의 소말리아해적 재판의 분석과 국제법적 검토”, 「해사법연구」, 23, pp.67-100.

서상범 외, “국가물류보안체제 고도화를 위한 물류보안표준참조모델 구축”, 「물류학학회지」, 제19권, 제2호, 2009, pp.71-90.

성낙청, “AEO 공인 제도의 D사 적용 방안을 중심으로”, 서경대학교 석사학위논문, 2011.

안광, 김인철, 김철승, “최신 정보통신기술을 활용한 해양사고 예방방안”, 해양환경안전학회 추계학술발표회, 2014.

안재덕, 이기욱, “우리나라 물류보안의 문제점 개선 방안 제안 및 분석”, 「한국콘텐츠학회논문지」, 제10권, 제2호, 2010, pp.352-360.

안재진, “국경안전 및 무역원활화를 위한 미국 및 EU의 공급망 보안제도 연구”, 「관세학회지」, 제8권, 제3호, 2007, pp.21-48.

양정호, “글로벌 기업의 공급사슬보안 및 위험관리전략에 관한 연구”, 「경영과 정보연구」, 27, 2008, pp.149-172.

이은방, “해양보안위협 대응을 위한 선박보안시스템에 관한 연구”, 「해양환경안전학회지」, 제9권, 제1호, 2003, pp.17-23.

정봉민, 「한중 물류보안 협력 증진방안 연구」, 한국해양수산개발원 단행본, 2008.

주종광, 김정환, 박성태, 이은방, “해양안전 보안의식에 관한 기초 연구”, 해양환경안전학회 학술대발표대회 논문집, 2005, pp.1-6.

최재선 외, “국가물류보안 체제 확립방안 연구(I)”, 한국해양수산개발원, 2006, pp.19-20.

허윤석, “국제물류보안 강화에 따른 공급사슬 위험관리 및 지향성이 국제무역업체의 성과에 미치는 영향에 관한 연구”, 성균관대학교 석사학위논문, 2013.

황의찬, “Logistics Security Assessment of Incheon Port”, 2009.2.

<외국 문헌>

Atkinson William(2001), "Gaining Supply Chain Visibility", *SCMR*, Vol. 5. Issue 6, Special Supplement, November.

Banomyung Routh(2005), "The impact of port and trade security initiatives on maritime supply chain management", *Maritime Policy Management*, Vol.32. No.1, pp.3-13.

Barnes Paul and Oloruntoba Richard(2005), "Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management", *Journal of International Management,* pp.519-540.

Christopher S. Tang, "Robust strategies for mitigating supply chain disruptions", *International Journal of Logistics*, 9(1), March, 2006, pp.33-45.

Closs David J. & Garrell Edmund F Mc(2004), *Enhancing Security throughout the Supply Chain*, IBM Center for The Business of Government.

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

Cranfield School of Management(2002), "Supply Chain Vulnerability", report on behalf of DTLR, DTI and Home Office.

Cranfield School of Management, "Creating Resilient Supply Chains: A Practical Guide", report on behalf of the Department for Transport, 2003.

David Closs, Ph.D et al., "Defending the food supply chain participant summary", U.S Department of Homeland Security, 2008.01

David J. Closs & Edmund F Mc Garrell, *Enhancing Security throughout the Supply Chain*, IBM Center for The Business of Government,

April 2004, p.37.

Donald Waters, *Supply Chain Risk Management*, KOGAN PAGE, 2007, p.7

Hau L. Lee and Michael Wolfe, "Supply Chain Security without Tears", SCMR, Jan/Feb, 2003, p.14.

Hau L. Lee and S. Whang, "Higher Supply Chain Security with lower cost: Lessons from total quality management", *International Journal of Production Management*, Vol. 96, 2005, pp.289-300.

ISP, *Specification for Security Management Systems for the Supply Chain*, 2007.

John F. Frittel, "Port and Maritime Security: Background and Issues", *Military Technology,* Nov. 2006, pp.88-94.

Kevin B. Hendrick and R. Vinod Singhal, "An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm", *Production and Operations management*, 2005, 14(1), pp.35-52.

M. Van de Voort, et al., "Improving The Security of the Global Sea-Container Shipping System", RAND Europe Report, MR-1695-JRC, 2003.

Making the Nation Safer, "The Role of Science and Technology in Countering Terrorism Committee on Science and Technology for Countering Terrorism of the National Research Council", The National Academies Press, 2002, p.214.

Ravi Sarathy, "Security and the Global Supply Chain", *Transportation Journal*, Fall 45, 4, 2006, p.30.

Vinh V Thai & Devinder Grewal, "The Maritime Security Management System: Perceptions of the international Shipping Community",

Maritime Economics & Logistics, 2007, pp.119-137.

William J. Stevenson, *Operations management*, McGraw-hill, 2005.

Yossi Sheffi and James B. Rice, "A Supply Chain View of the Resilient Enterprise", *Sloan Management Review*, Fall 2005, p.47.

Yossi Sheffi, "Resilience Reduces Risk", *Logistics Quarterly*, Vol.12, Issue 1, March 2006, p.13.

Yossi Sheffi, "Supply Chain Management under the Threat of International Terrorism", *IJLM*, Vol. 12, No. 2, 2001, pp.4-6.

<인터넷 자료>

광양관세사 홈페이지 (http://www.kyca.co.kr)

국제물류보안 동향과 인증제도 비교 웹사이트(http://sekujung.blog.me)

항만물류안전의 확보를 위한 보안제도에 관한 고찰 웹사이트 (http://www.hanyang.ac.kr)

기술자산 보호협회 홈페이지(http://korean.jupiterexp.com)

CR. Hamilton, The case for holistic security: The integration of information and physical security as an element of homeland security, 2004(www.riskwatch.com/Press/Holistic_Security_10-03.pdf)

S. Wiederin, D. Wurster, RS Hoefelmeyer and T. Phillips, The true meaning of security, 2002 (www.rrtidd.com/webQuest/shared/true%20Meaning%20of%20Security.pdf)

感謝의 글

“세상에서 가장 지혜로운 사람은 배우는 사람이고,
세상에서 가장 행복한 사람은 감사하며 사는 사람이다.”

지혜로운 사람으로 살아가고 싶은 마음과 배움에 대한 길고 긴 갈망으로 시작하였습니다. 그 동안 다사다난한 시간 속에서도 늘 따뜻한 마음으로 지켜봐 주시고 도와주신 분들에게 진심으로 감사 드립니다.

아낌없는 지도와 사랑을 베풀어 주신 우리 교수님.. 신영란 교수님!
평생 잊지 않겠습니다. 은혜를 갚을 줄 아는 됨됨이가 된 사람으로 살아가겠습니다. 글로는 다 표현할 수 없을 만큼 감사 드립니다.
진심으로 응원해주신 김환성 교수님, 김율성 교수님! 학문에 대한 깊이와 열정을 본받고 싶습니다. 감사한 마음 잊지 않겠습니다.

24기 동기님들! 사랑합니다.
항상 더 착하게 살아가겠다는 성지혜님! 그 착한 마음이 고스란히 내게 전해졌어.. 인연의 소중함을 잊지 않을게!

항상 감사한 마음으로.. 세상에서 가장 행복한 사람으로..

권유성 올림.