Journal of Korea Port Economic Association, Vol.27, No.2, 2011, 333-354

국제물류보안 인증제도 동향 및 시사점에 관한 연구

고현정*

A Study on the Implications and Trends of Logistics Security Assurance Programs for International Trade Facilitation

Hyunjeung Ko

Abstract : After the terrorist attack of 9/11 on the USA, the security concern to global trade has been raised. In particular, the USA has actively promoted a series of initiatives and rules such as CSI, 24 hour rule, C-TPAT, and so on in the area of logistics activities, which aimed to better protect the country against the potential terrorist threats. While implementing such schemes called as a multi-layed logistics security strategy, a large number of countries trading with USA are facing with the issues of additional time and costs for inspecting cargos in their logistics facilities. As a result, most countries all over the world have sought a way to minimize the impacts from such strategy. The Korea also is preparing the several security programs operated by various ministries, which are aiming to not only improve the efficiency of trade flows but also to ensure supply chain security. However, many companies are expressing the inefficiency of operating such programs. Thus, this paper analyzed several global supply chain security programs currently adopted by international organizations(ISO, WCO, and IMO) and major countries(USA, EU, and Singapore) and suggested a guideline for developing the national logistics security system.

Key Words : Supply Chain Security, Authorized Economic Operator, C-TPAT

▷ 논문접수: 2011.01.30 ▷ 심사완료: 2011.03.09 ▷ 게재확정: 2011.03.24
* 군산대학교 물류학과 조교수, hjko@kunsan.ac.kr, 063)469-4802

Ⅰ. 서 론

2001년 미국에서 발생한 9·11 항공기 테러사건은 국제교역 보안에 관한 관심을 증대시켰다. 특히 세계는 경제의 개방화 및 상호 의존성이 심화됨에 따라 테러리스트가 국가 간 교역활동을 악용하여 대상국의 인명 또는 재산적 손실을 가하는 가능성에 우려하고 있다. 피해 당사국인 미국은 테러 위협에 대해 다층적 방어 전략을 추진하면서 행정조직을 대폭 개편하여 국토안보부(DHS)[1]를 설치하고 CSI, 화물정보 24시간 전 신고, SAFE Port Act, 9/11 테러대책이행법 등 다양한 물류보안 제도를 마련하였다. 또한 테러활동이 전 세계적으로 확대되면서 국제기구 및 세계 각국과 공조하면서 사실상 글로벌 물류보안체계 구축을 주도하고 있다.

글로벌 물류보안체계는 항공 또는 해상운송의 단순한 운송수단 보안에서 국제교역 화물의 제조, 운송, 보관, 정보 등의 공급사슬관리(Supply Chain Management) 전 과정으로 확대되고 있다. 이는 보안관리 대상의 범위를 확대시키면서 국제교역 흐름의 효율성을 저하시키는 요인으로 작용하고 있다. 즉 보안을 강화하기 위한 점검, 확인, 검사 등의 추가적인 절차가 요구됨에 따라 보이지 않는 교역장벽으로 작용하기 때문이다. 그러나 물류보안을 효율적으로 관리하면 화물의 도난 및 손실감소, 가시성 향상, 배송시간 정확성 향상, 재고관리 향상, 고객만족도 향상, 효율적인 통관업무 수행, 물류관리 향상 등의 효과도 동시에 달성할 수 있다는 긍정적인 연구결과가 제시되기도 하였다(Barchi et al, 2006).

공급사슬에는 생산자와 최종소비자를 연계하는 다양한 주체들이 활동하고 있는데, 그 주체들은 운송업자, 창고운영자, 3PL, 은행, 관세사 등의 민간기업 뿐만 아니라 세관, 항만당국, 출입국관리국 등의 정부기관도 포함된다. 이처럼 공급사슬보안은 개별기업의 자체적 보안뿐만 아니라 상호 연계된 기업의 보안상황도 중요하므로 기업 간 상호협력이 필수적이다. 그러나 현실적으로 모든 교역화물에 대해 보안점검을 실시하는 것은 많은 비용과 시간이 소요되므로 비효율적일 수밖에 없다. 이러한 물류보안 강화의 비효율성을 극복하고 교역의 원활화를 추구하는 방안이 물류보안 인증제도의 활용이다. 미국은 교역흐름의 원활화 방편으로 2002년 물류보안 인증제도인 C-TPAT[2] 프로그램을 추진하면서 국제기구와 각국의 관심을 유도하고 있다. 국제기구인 세계관세기구(WCO), 국제표준화기구(ISO), 국제해사기구(IMO)는 글로벌 차원에서 물류보안 인증제도를 도입하고 있고, EU, 싱가포르 등 세계 각국도 자국의 실정에 맞는 물류보안 인증제도를

1) 부시 대통령이 의회의 의결을 거쳐 행정부로 이송된 국토안보부(Department of Homeland Security) 설립에 관한 법률에 최종 승인하였고, 이는 연안경비대와 관세청의 기능을 통합하였다.

2) Customs-Trade Partnership Against Terrorism.

마련하고 있다. 특히 우리나라는 강화되고 있는 국제물류보안 제도에 대처하고자 국토해양부, 관세청, 그리고 지식경제부는 부처별로 물류보안 인증제도를 운영하고 있다.

그러나 국내 인증제도에 참여하는 실제적 당사자인 기업은 각 기관별로 운영되는 물류인증에 투자되는 시간과 비용의 중복 문제점을 지적하고 있다. 물류보안 인증제도의 운영취지는 글로벌 차원의 보안강화에 따른 화물흐름의 지체현상을 필연적으로 겪게 되는 기업을 지원하자는 의도인 바, 기업의 부담을 최소화하는 통합된 국가 물류보안제도의 마련은 중요하다고 할 수 있다. 따라서 본 연구는 국제기구 및 주요국의 인증제도를 분석하고 시사점을 제시하여 국내 물류보안 인증제도의 효율적 운영방향을 설정하는데 그 목적이 있다.

물류보안과 관련된 연구를 살펴보면 물류보안 제도에 관한 설명과 동향을 소개하는 내용이 대부분이다(Bames and Oloruntoba, 2004; Ereara et al., 2003; Banomyong, 2005; Hesse and Charalambous, 2004; Roach, 2004; Barch et al., 2006; Thai and Grewal, 2007). 하지만 물류보안 인증제도를 다룬 연구는 극소수에 불가하다. 특히 최재선 등(2006)이 한국해양수산개발원에서 정책과제로 「국가물류보안체제 확립방안」에 대한 연구를 수행하였다. 주요 내용은 글로벌 물류보안제도의 현황을 제시하면서 국가물류체제 구축의 방향을 제시하였다. 그 후 2007년 제2차 정책과제로 제1차 내용을 바탕으로 국내의 대응방안을 거시적 측면에서 제시하였다. 안재진(2007)은 미국과 EU의 AEO[3] 제도를 소개하면서 우리나라 실정에 맞는 한국형 AEO제도 도입의 필요성을 피력하였다. 또한 2008년에는 일본의 AEO추진 동향과 방법을 제시하면서 글로벌 기준에 맞는 제도 도입의 중요성을 제시하였다. 송선욱(2008)은 국내 관세청이 수출입안전관리 우수공인업체(AEO) 제도의 국내도입을 준비하는 시점에 서 호주와 EU의 사례를 이용하여 한국형 AEO 제도의 효과적인 운영방향을 제시하기도 하였다.

그러나 기존의 연구는 관세청에서 추진되고 있는 AEO제도를 위주로 국내의 인증제도 운영방향만 제시하고 있는 한계점을 갖고 있다. 이와 달리 본 연구에서는 최근 기업들이 부담으로 인식하고 있는 다양한 부처별 인증제도의 운용에 대한 정책적 해결방안을 위한 시사점을 도출하는데 중점을 두고자 한다.

Ⅱ. 국제기구의 물류보안제도

1. 국제표준화기구의 ISO 28000

3) Authorized Economic Operator.

(1) 개요

ISO 28000은 국제표준화기구(International Organization for Standardization: ISO)에 의해 제정된 물류보안 인증제도이다. 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 28000[4] 형태로 공급사슬 보안경영시스템에 대한 국제표준을 제공한 후 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. 즉, 조직이 지속적으로 보안환경을 평가하고 충분한 보안조치가 행해지고 있는지의 여부와 법제도 및 강제적 요구사항이 조직에 끼칠 영향을 지속적으로 모니터링하면서 문제점을 개선하는 것이다.

<표 1> ISO 28000 시리즈

구분	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: ISO, Specification for Security Management Systems for the Supply Chain, 2007

(2) 보안기준 주요 내용

ISO 28000의 보안기준은 일반요구사항, 보안경영방침, 보안리스크 평가 및 기획, 실행 및 운영, 점검 및 시정조치, 경영검토 및 지속적 개선의 6가지 영역으로 구성되어 있다. 첫째, 일반요구사항은 조직이 보안위험을 식별하고 그 영향을 통제하는 한편, 보

4) ISO/PAS는 ISO Publicly Available Specification의 약어이며, PAS란 ISO의 전문가들이 모인 위원회에서 잠정적으로 합의한 협약으로 그 후 재검토 과정을 거쳐 회원국의 50%이상이 동의하면 국제 표준안으로 채택된다.

안 위험을 최소화하는 보안관리시스템을 구축하고 실행·유지·개선하는 의무를 명시하고 있다. 둘째, 보안경영방침은 조직의 최고경영자가 조직의 보안관리 방침을 수립·승인하고 문서화하여 관리해야 하는데, 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 보안경영시스템에 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 보안경영시스템의 변경과 관련된 의사결정 및 조치사항도 관리되어야 한다.

2. 국제관세기구의 WCO Framework

(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 막힘

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

<표 2> 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 민간협력(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
SAFE Framework에 대한 결의안	

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 테러위험을 최소화하기 위해 위기관리와 복구절차를 마련하여 특이한 상황에 대비해야 하는 내용이다.

3. 국제해사기구의 ISPS Code

(1) 개요

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 고속 여객선을

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.

(2) 보안기준 주요 내용

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.

i) 보안2등급에서 접근지점이나 경계 장벽을 보호하는 인원을 추가로 할당 하였는가?
ii) 보안2등급에서 항만시설 접근지점의 수를 제한하는 조치를 수립하였는가?
iii) 보안2등급에서 항만시설 접근지점을 통한 이동 저해조치를 수립하였는가?
iv) 보안2등급에서 인원, 휴대품 및 차량의 검색빈도를 증가하는 조치를 하였는가?
v) 보안2등급에서 항만시설에 검증 가능한 정당성을 제시하지 못하는 방문자의 접근을 거부하였는가?
vi) 보안2등급에서 해상 보안을 강화하기 위한 순찰선을 사용하는 조치를 하였는가?

III. 주요국의 물류보안 인증제도

1. 미국의 C-TPAT

(1) 개요

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 보안 등의 항목에 대해 종합적인 평가를 받게 된다.

C-TPAT은 인증등급을 3단계로 구분해서 운영되고 있는데, 등급마다 차등적인 통관혜택을 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

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. 둘째, 컨테이너 및 트레일러 보안은 화물의 선적장소에서 운송수단의 보안 무결성(integrity)을 확보하기 위하여 무권한(unauthorized) 물체 및 사람의 진입을 차단하는 절차를 마련해야 하는 내용이다. 이를 위해 ISO

5) 업종별 특성에 따른 차별적인 C-TPAT Minimum Security Criteria 또는 C-TPAT Security Guideline에 의해 적용받고 있으며, 점차적으로 Guideline은 Minimum Security Criteria로 전환되고 있다.

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, 건물구조, 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 규칙적으로 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 보안상황을 인식하도록 훈련을 받아야 한다.

2. EU의 AEO

(1) 개요

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, 국제 공급사슬 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, 포워

더, 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-관세절차 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.

<표 3> AEO 형태별 혜택

AEO 혜택	AEO-관세절차 간소화	AEO-보안 및 안전	AEO-관세절차 간소화/보안 및 안전
세관절차 간소화	O		O
물리적 및 서류심사 횟수 축소	O	O	O
화물검사 필요시 우선권 부여	O	O	O
검사의 장소 선택권 부여	O	O	O
재검사 정보 우선적으로 제공		O	O
세관신고서의 데이터 간소화		O	O

자료: EC, Authorized Economic Operators, June 2007.

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, BSKM[6]자격을 부여하여 기업경쟁력 강화지원, BSKM의 글로벌 인지도 지원, 미국 등과의 타 국가와의 상호인증 참여, 운송 보험료의 감소 등의 혜택을 부여하고 있다.

(2) 인증기준 주요 내용

EU의 AEO 인증을 위한 평가기준은 5가지 영역, 즉 기업정보, 법규준수 기록, 기업회계 및 물류시스템, 재정능력, 안전 및 보안요구로 구성되어 있다. 특히 평가 항목가운

6) BSKM : British Standards Kite Mark.

데 안전 및 보안요구와 기업회계 및 물류시스템 영역에서 기업이 물류보안 국제인증인 ISO 28000, ISPS Code[7], TAPA[8] 인증을 보유한 경우 AEO 인증 심사에서 동일 평가항목에 대하여 중복심사를 가능한 축소하여 심사 효율성을 추구하려는 부분이 특징이라 할 수 있다.

첫째, 기업정보 영역은 기업규모와 관세 관련 통계에 관한 항목을 포함한다. 기업규모는 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 정보공유 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 방지하는 조치를 마련하는 것이다. 이러한 조치는 화물단위[9], 물류절차, NFR[10], 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.

---

7) ISPS Code : International Code for the Security of Ships and Port Facilities.
8) TAPA : Technology Asset Protection Association Certificate.
9) 화물단위는 화물 운송에 사용되는 컨테이너, 탱커, 벤, 화물자동차, 운송기기, 파이프라인 등을 의미한다.
10) NFR은 Non-Fiscal Requirement로 수출입 금지 또는 제한품목에 대해 허가유무와 이중사용 물품을 거래유무, 통상금지 물품의 거래 유무를 의미한다.

<표 4> 안전 및 보안요구 평가항목과 타 인증제도의 연계성

구분	내용	ISO 관련 참고사항
Section V : 안전 및 보안 요구	자체 보안평가(Security assessment conducted by the economic operator(self assessment)	ISO 9001:2001, section 5.5.1 ISPS Code ISO/PAS 28001:2006, section A.3.3, A.4.2
	출입통제(Entry and access to premises)	ISO/PAS 28001:2006, section A.3.3 ISPS Code
	물리적 보안(Physical security)	ISO/PAS 28001:2006, section A.3.3, ISPS Code
	화물절차(화물단위, 물류절차, NFR, 물품반입, 물품보관, 물품생산, 물품적재)	ISPS Code ISO 9001:2001, section 6.2.2 ISO/PAS 28001:2006, section A.3.3 ISO/PAS 17712 ISO 9001:2000, section 7.4 TAPA(Technology Asset Protection Association Certificate)
	비즈니스 파트너의 보안요구(Security requirements business partners)	ISO/PAS 28001:2006, section A.3.3
	인력보안(Personnel security) 및 외적 서비스(External services)	ISO/PAS 28001:2006, section A.3.3

자료: EC, Authorized Economic Operators, June 2007.

3. 싱가포르의 STP

(1) 개요

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

<표 5> STP 프로그램 구조

목차	내용
서문	STP Guidelines와 STP Criteria에 대한 개요
보안 관리시스템	기업은 자사의 공급사슬 보안 기준 및 이행을 개발하고, 문서화, 이행, 유지, 그리고 리뷰하기 위한 시스템을 구축
리스크평가	기업은 자사의 운영 프로세스와 공급사슬에 대한 리스크 평가를 실시해야 하고, 공급사슬에서의 자사 운영 프로세스의 리스크와 취약요소를 경감
보안기준	STP와 STP-Plus 인증을 위한 8가지 보안충족 요소
부록 A : STP 자격에 대한 보안기준 부록 B : STP-Plus 자격에 대한 보안기준	건물보안과 출입통제, 인력보안, 비즈니스 파트너 보안 화물보안, 운송보안, 정보 및 정보기술 보안, 사고관리와 조사, 위기관리 및 사고회복

자료: Singapore Customs, Secure Trade Partnership : Guidelines and Criteria, 2008.

싱가포르는 공급사슬보안의 중요성 인식 및 STP 프로그램 확산을 위해 무료 STP 과정 운영, 일대일 기업컨설팅 등의 다양한 프로그램을 운영하고 있다. 기업지원은 세관과 타 기관, 즉 EDB[11](Economic Development Board) 또는 SPRING Singapore[12]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[13]를 통한 재정적 지원, CMC[14]를 통한 컨설팅 및 인증비용 지원 등을 제공하고 있다.

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

12) 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 국가경쟁력강화 및 무역촉진 등의 업무를 수행한다.

13) 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.

14) 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.

(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. 첫째, 시설보안과 접근통제는 담장(wall or fence)을 적소에 설치하여 기업 시설물에 대한 내외부의 무단침입을 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.

IV. 국내 물류보안체계 구축에 주는 시사점

1. 국제기구의 인증제도

(1) 미국의 물류보안 강화 정책에 협력

미국은 9.11 테러 이후 자국의 보안을 강화하기 위한 전략으로 다층적 방어책을 적용하여 복합적으로 테러에 대응하는 정책을 추진하고 있다. 이러한 미국의 물류보안 강화 정책에 따라 IMO, WCO, ISO 등의 국제기구는 각각 국제 물류보안 제도를 마련하고 있다. 따라서 이는 세계 각국들이 국제기구의 보안제도를 분석하여 자국에 도입하는 노력을 적극적으로 추진해야 향후 보안 강화에 따른 자국의 불이익을 최소화하면서 국가 경쟁력을 강화할 수 있다는 의미이다.

(2) 물류보안 인증제도, 국가를 대표하는 책임기관 필요

국제기구의 물류보안 인증제도를 보면 궁극적으로 국가 간 상호인증을 통해 자국의 인증제도를 국제적으로 확대하는 체계이다. 즉, 국가 간 상호인증을 보증하는 자국의 정부를 대표하는 주관기관이 필요하며, 이 주관기관은 AEO를 승인하고, 주기적 감시를 통해 AEO의 자격이 미달할 경우 정지, 취소와 같은 관리 기능을 수행해야 한다. 따라서 이는 각국이 주관기관을 선정하고 기업의 AEO지위를 지속적으로 감찰하고 유지·관리하여 국제 공조체제를 구축하는데 협력해야 한다는 의미이다.

(3) ISO 28000, 물류보안을 기업의 경영 측면에서 접근

ISO 28000 시리즈는 산업전반의 공급사슬 보안확보를 대상으로 하며, 개별기업은 자체적으로 보안경영시스템을 구축하여 국제적으로 상호 연계될 수 있는 규격이다. 조직은 지속적으로 보안환경을 평가하고 충분한 보안조치가 행해지고 있는지의 여부와 법제도 및 강제적 요구사항이 조직에 끼칠 영향을 파악하는 것이 필요하다. 따라서 타 인증제도와 달리 구체적인 평가기준을 설정하는 것이 아니라 기업의 품질관리, 마케팅, 재무관리 등의 기능과 유기적으로 연계되어 보안경영시스템을 구축하는 것이다.

(4) 국제기구 보안규정, 상호 보완적으로 활용하는 전략 필요

국제기구의 각 보안규정은 각각의 장단점을 보유하고 있는바, 이를 상호 보완적으로 연계될 때 효율적인 글로벌 공급사슬보안 체계가 구축되어 시너지가 효과가 발생될 수 있다고 판단된다. 국제기구의 물류보안 제도의 운영적 특징을 살펴보면, ISO 28000의 경우 조직 자체적으로 보안경영시스템을 구축하여 운용하는 것으로 기업경영의 총체적 최적화 측면에서 물류보안이 고려되어지는 것으로 법적 강제성과 투명성이 약하다고 할 수 있다. 반면, WCO Framework는 국제상거래의 원활화 및 보안확보를 위해 법적 근거에 따라 공급사슬보안이 다루어지고 있는 바, 기업경영 측면보다 특정 기준 준수에 주안점을 주고 있다. 또한 ISPS Code는 국제법상 강제규정으로 작용되고 있으며 공급사슬 전반의 보안확보 보다 항만시설 및 선박에 대한 보안확보로 제한되어 있는 것이 특징이다.

2. 주요국의 인증제도

(1) 물류보안 평가기준에 따라 다양한 AEO 종류 운영

미국 C-TPAT의 AEO 인증은 1단계, 2단계, 3단계로 나누고, 각 단계에 상응하는 혜택을 부여하고 있다. EU 또한 인증수준에 따라 관세행정 간소화, 보안 및 안전, 그리고 모든 혜택을 누릴 수 있는 관세절차간소화-보안 및 안전으로 나누어 기업의 실정에 맞게 AEO 인증을 선택하게 하고 있다. 싱가포르는 2가지 인증 종류를 운영하고 있는데, STP-Plus가 STP 보다 높은 수준의 기준이 적용되며 타국과의 상호인증이 적용되는 단계이다.

(2) 각국의 물류보안 평가기준, 자국의 실정에 따라 상이

미국의 C-TPAT은 기업특성에 따라 조금씩 차이가 있지만 일반적으로 9가지 평가항목으로 구성된 보안 및 안전요구에 주안점을 두고 디자인되어 있다. 그러나 EU의 AEO 평가항목은 관세행정과 보안 및 안전에 관한 내용이 복합적으로 구성되어 있다. 한편, 싱가포르 STP는 보안관리시스템, 리스크평가, 그리고 보안 및 안전기준(8가지 세부항목)으로 구성되어 있다. 그 특성을 보면 관세행정보다 기업경영의 효율성에 주안점을 두고 있으며 ISO 28000의 장점을 도입하여 모든 기업에 적용가능 하도록 하고 있는 것이 특징이다.

(3) 세관당국, 각국의 AEO의 주관기관으로 활동

미국은 자국의 물류보안을 강화하는 일환으로 관세청의 기능을 확대하여 이를 전담하는 CBP(Customs and Border Protection)를 창설하였다. CBP는 국토안보부의 5가지 기능 가운데 국경 및 수송부문 보안국(BTS Bureau)에서 기존의 관세청이 수행하던 화물 및 여행자 휴대품 검사와 관세 부과, 이민 귀화국 업무 중 출입국심사와 국경순찰, 동식물 검역소의 검사검역 업무 등을 통합하여 관리영역을 확대한 조직이다. 따라서 CBP의 대응기관인 각국의 관세당국은 자국의 물류보안 제도를 주도하는 부서로 진화하게 되고, 인증제도 운영의 핵심기관으로써의 역할을 담당하게 되었다. 인증제도의 중요한 역할은 AEO의 승인, 정지, 취소와 같은 권한이라 할 수 있다.

(4) 각국 AEO 제도, 국제표준과 연계하여 운영 효율성 추구

EU의 AEO 제도에는 AEO 지원자가 보유한 인증서, 전문가의 견해 등에 대한 내용을 AEO 인증 시 참고하도록 하고 있다. 특히 국제인증으로 ISO 기준(ISO 9001, 14001, 20858, 28000, 28001, 2004)과 ISPS Code 등이 해당된다. 하지만 ISO 인증이 자동적인 AEO 평가기준의 충족을 의미하지는 않는다고 언급하고 있다. 그 이유는 특정 평가기준을 충족하지만 타 기준을 충족하지 않을 수도 있기 때문에 세관이 종합적으로 검토한 후 최종 결정을 내린다는 것이다. 또한 국제기구(IMO, UNECE, ICAO 등)의 기준도 부분적으로 AEO의 평가기준을 충족하는 것으로 언급하고 있다.

싱가포르의 경우를 보면, STP 프로그램 운영에서 기업이 보유한 인증서에 대한 참조를 언급하고 있다. 즉, STP 프로그램이 ISPS, TAPA(Technology Asset Protection Association Certificate)등의 인증을 대체하는 역할이 아니라 공급사슬 보안기능을 보완하여 더욱 강화하는데 도움을 주는 것으로 언급하고 있다.

(5) 각국 AEO 제도, 기업의 부담 최소화 추구

EU의 경우 회원국 세관은 중소기업에 대한 특수 상황을 적극 고려하도록 지적하고 있다[15] 즉 AEO 평가기준은 모든 기업에게 동일하게 적용되어야 하지만 기업의 규모, 복잡성, 취급제품 등에 따라 평가기준의 준수성(compliance)을 충족하는 방식(means)은 다를 수 있다는 것이다. 그리고 싱가포르는 정부차원에서 재정적 지원을 제공하면서 기업의 부담을 감소시키면서 STP 인증제도의 활성화를 추진하고 있다. 국가 산업발전을 지원하는 EDB(Economic Development Board)와 SPRING Singapore를 활용해 세관의 STP 제도를 지원하고 있다. EU, 미국 등은 인증기업에게 직접적 재정지원보다 실질적

15) CCIP의 Article 14a (2) : "the customs authorities shall take due account of the specific characteristics of economic operators, in particular of small and medium sized companies.

인 통관혜택을 부여함으로서 기업의 참여 및 투자비용을 상쇄할 수 있는 체계를 추진하고 있다.

V. 결론 및 정책적 시사점

우리나라는 동북아 물류허브화 정책추진 및 물류정책기본법에 물류보안시책을 마련하는 등 공급사슬보안에서 국가 이미지를 제고하고 국가경쟁력을 강화하기 위한 체계적인 대응전략을 마련하고 있다. 이를 위해 본 연구는 국가 공급사슬보안체계 구축의 기본방향을 크게 3가지, 즉 글로벌 수준의 공급사슬보안체계 구축, 국내적으로 효율적 운영체계 구축, 국가적 차원의 지원체계 구축을 제시하고자 한다.

글로벌 수준의 공급사슬보안체계 구축의 필요성은 공급사슬보안이 국제적인 화물의 흐름과 연계된 거대하고 복잡한 시스템을 통제 및 관리해야 하는 특성이 있는 바, 국가간 요구사항을 충족할 수 있는 글로벌 수준의 공급사슬보안 체계를 구축하는 것이 요구된다고 할 수 있다. 글로벌 기준을 충족하지 못한 공급사슬보안 체계는 국제적으로 통용되지 못하고 자국에만 한정되어 국제적인 신뢰를 확보할 수 없기 때문이다.

국내적으로 효율적 운영체계 구축의 필요성은 강화되고 있는 글로벌 공급사슬보안제도는 테러 예방이라는 원론적인 목적을 달성하기 위해 보안강화와 국제무역의 원활화라는 두 가지 상충적인 요소를 조화롭게 연계하는 지혜가 필요하다고 할 수 있다. 이를 위해 각국은 첨단장비 개발 및 인증 제도를 활용하여 원활한 국제교역의 흐름을 보장하고자 노력하고 있다. 뿐만 아니라 정부와 민간 간 긴밀한 협력 체제를 형성하여 보안을 강화하는 대안으로 활용되고 있기 때문에 효율적인 연계전략이 중요하다고 할 수 있다. 특히 공급사슬보안제도는 물류흐름의 특정구간에만 적용되는 것이 아니라 공급사슬 전 과정에서의 보안확보가 중요하기 때문에 정부 부처를 포함하여 다양한 이해당사자가 참여하기 때문에 이들 간의 상호연계 및 협조가 중요하다. 공급사슬 전 과정에서의 전문인력을 양성하여 국가 산업 전 영역에서 자체적이고 자발적인 보안경영시스템이 가동되도록 하는 정책적 방향의 수립이 필요다고 판단된다. 또한 보안 사고나 사건이 발행한 경우 그 영향을 최소화는 위기관리 및 복원에 필요한 전문인력도 양성되어야 한다.

국가적 차원의 지원체계 마련은 공급사슬보안은 9.11 테러라는 다른 나라에서 발생한 외생 변수로 인해 국제적으로 도입되고 있는 제도라 할 수 있다. 따라서 국가적 차원에서 지속적 관심과 지원이 당연시 되며 국가적 차원의 다양한 지원체계가 마련되어야 한다. 글로벌 공급사슬 보안강화는 정부차원의 다양한 시설 및 검사기 도입, 민간기업

의 보안시설 구축 등의 하드웨어 구축뿐만 아니라, 경영시스템 전환을 위한 다양한 컨설팅 비용이 요구되기 때문이다. 즉, 정부 및 민간 기업에 대해 비용적인 부담을 주고 있으며 이를 효율적으로 해결하는 방안을 마련하는 것이 필요하다. 특히 중소기업의 경우 독자적으로 보안시스템을 구축하는 것은 재정적으로 많은 부담이 있는 바, 국가 보안체계의 효율적 운영을 위해 이를 지원하는 방안도 마련하는 것이 요구된다.

결론적으로 본 연구는 국제기구 및 주요국의 인증제도를 분석하고 시사점을 도출하여 국가 공급사슬보안체계 구축의 기본방향을 제시하였다. 그러나 우리나라에서 추진되고 있는 물류보안 인증제도의 장단점이 반영되지 못한 한계점이 있다. 따라서 향후 물류보안 인증제도의 실제 사용자인 기업들의 의견을 반영하여 국내제도의 개선방안을 제시하는 후속 연구가 필요하다고 판단된다.

참고문헌

송선욱, “관세법상 수출입 안전관리 우수공인업체 제도의 효과적 운영방향”, 『관세학회지』 제9권 제3호, 2008, 1-27.

송선욱, “일본의 AEO제도 추진 시사점과 우리나라 추출입안전관리 우수공인업체 추진 방향”, 『관세학회지』 제9권 제1호, 2008, 21-48.

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

최재선, 목진용, 황진회, 고현정, 『국가 물류보안체제 확립방안 연구 I』, 한국해양수산개발원, 2006.

최재선, 목진용, 황진회, 고현정, 김민수, 『국가 물류보안체제 확립방안 연구 II』, 한국해양수산개발원, 2007.

Banomyong, R., “Impact of Port and Trade Security Initiatives on Maritime Supply-Chain Management”, *Maritime Policy and Management*, Vol.32, Jan-Mar 2005, 3-13.

Barchi, P.G., Bhat G. and Sept L., *Innovators in Supply Chain Security : Better Security Drives and Business Value*, Stanford University, July 2006.

Barnes, P. and Oloruntoba, R., “Assurance of Security in Maritime Supply Chain : Conceptual Issue of Vulnerability and Crisis Management”, *Journal of International Management*, Vol.11, 2005, 519-540.

Cariel P. and Talley W., “The Security Incident Cycle of Port”, *Maritime Economics & Logistics*, Vol.8, 2006, 267-286.

Erera, A., Kwek, H., Goswami, N., White, C. and Zhang, H., “Cost of Security for Sea Cargo Transport”, The Logistics Institute-Asia Pacific, May 2003.

European Commission, *Authorized Economic Operators*, June 2007.

Hesse, H. and Charalambous, N., “New Security Measures for the International Shipping Community”, *WMU Journal of Maritime Affairs*, Vol.3, 2004, 123-138.

International Organization for Standardization, *Specification for Security Management Systems for the Supply Chain*, 2007.

Roach, J.A., “Initiatives to Enhance Maritime Security at Sea”, *Maritime Policy*, Vol.28, 2004, 41-66.

Singapore Customs, *Handbook on Secure Trade Partnership*, May 2007.

Thai, V. and Grewal, D., “The Maritime Security Management System : Perceptions of the International Shipping Community”, *Maritime Economics & Logistics*, Vol.9, 2007, 119-137.

국문요약

국제 물류보안 인증제도 동향 및 시사점에 관한 연구

고현정

2001년 미국에서 발생한 9·11 항공기 테러사건은 국제교역의 보안에 관한 관심과 우려를 증대시켰다. 그리고 미국은 테러 위협에 대해 다층적 방어 전략을 추진하면서 행정조직을 대폭 개편하여 국토안보부를 설치하고 CSI, 화물정보 24시간 전 신고제도, SAFE Port Act, 9/11 테러대책이행법, C-TPAT 등 다양한 물류보안 제도를 마련하였다. 그 결과 전 세계적으로 물류보안 제도가 강화되고 있다. 우리나라는 동북아 물류허브화 정책추진 및 물류정책기본법에 물류보안시책을 마련하는 등 공급사슬보안에서 국가 이미지를 제고하고 국가경쟁력을 강화하기 위한 체계적인 대응전략을 마련하고 있다. 하지만 국내 인증제도에 참여하는 실제적 당사자인 기업은 각 기관별로 운영되는 물류인증을 획득하기 위해 투자되는 시간과 비용의 중복 문제점을 지적하고 있다. 물류보안 인증제도는 국가차원의 보안강화에 따라 화물흐름의 지체현상을 필연적으로 겪게 되는 기업을 지원하자는 의도인 바, 기업의 부담을 최소화하는 통합된 국가 물류보안제도의 마련은 중요하다고 할 수 있다. 따라서 본 연구는 국제기구 및 주요국의 인증제도를 분석하고 시사점을 제시하여 국내 물류보안 인증제도의 효율적 운영방향을 설정하고자 하였다. 그리고 국가 공급사슬보안체계 구축의 기본방향을 크게 3가지, 즉 글로벌 수준의 공급사슬보안체계 구축, 국내적으로 효율적 운영체계 구축, 국가적 차원의 지원체계 구축을 제시하였다.

핵심 주제어 : 공급사슬보안, 공인경제운영자, 물류보안인증, C-TPAT.