한국무역상무학회지 제54권
2012년 5월 pp. 45~80

논문접수일 2012.04.30
논문심사일 2012.05.13
심사완료일 2012.05.23

Incoterms® 2010상 수출입 당사자의 보안관련 의무에 관한 연구

양 정 호*

주제어 : 인코텀즈2010, 물류보안, 물류보안 인증, 수철통제

Ⅰ. 서 론

2001년 발생한 9/11 테러사태는 공급사슬 전반에 큰 혼란을 야기함으로써 기업들이 보안위험에 대한 공급사슬의 취약성을 인식하는 계기가 되었다.[1] 이

* 전주대학교 경영학부 조교수

1) 2002. 2. 18일 자 포천지에 따르면, 재고증가, 국경폐쇄, 리드타임 증가, 기타 9/11사태로 인한 보안조치들이 미국 공급사슬에 미친 영향은 연간 미화 1천 5백억 달러로 추산하고 있다.

를 계기로 세계 각국과 국제기구에서 물자의 안전한 흐름을 보장하기 위한 보안조치를 강화하면서 물류 공급망의 안전성을 확보하기 위한 물류보안이 세계 교역질서에 새로운 패러다임으로 정착되고 있다.

Incoterms® 2010은 강화된 글로벌 공급사슬 보안환경에서 공급사슬보안규정의 준수를 지원한다는 점에서 의의를 가진다. Incoterms® 2010에서는 수출입 당사자에게 수출입 화물의 보안에 관한 의무를 규정하고 있는 바, 이는 EU의 AEO제도나 미국의 C-TPAT, 10+2 규칙으로 알려진 수입자 보안신고프로그램(ISF: Importers Security Filling) 등 수출입 통관을 위한 사전 신고요건 등과 연관성을 지닌다. 가령, 미국의 수입업자들은 ISF 규정과 관련된 규제준수관리 프로세스의 실행에 있어서 어려움을 겪고 있다. 그 이유 중 하나는 해외 수출업자가 선적예정화물에 대한 24시간 전 사전신고 의무를 해태하거나 적기에 정보를 제공하지 않음으로 인해 발생한다. 이 경우 수입자에게는 ISF 위반 건당 미화 5,000 달러의 벌금이 부과된다. 이러한 결과를 피하기 위해서 그리고 신속한 통관절차의 보장을 통한 경쟁력 확보를 위해서는 보안관련 정보의 획득, 제공 및 관리에 있어서 수출입 당사자 간 긴밀한 협조가 필요하다. 하지만, 이러한 사항이 계약상 의무로 규정되지 않은 경우 거래 상대방이 보안관련 정보의 제공이나 필요한 지원을 하지 않음으로 인해 초래되는 불이익이나 추가적인 비용, 그리고 계약이행 지연에 대한 책임소재를 가리는데 어려움이 있다. Incoterms® 2010은 수출입 당사자인 매도인과 매수인에게 보관의 연속성을 유지하기 위한 정보(chain of custody information) 등 보안통관(security clearance)을 위한 관련 정보의 획득 및 절차를 이행하거나 상대방이 그러한 정보를 획득하거나 절차를 이행하는데 필요한 협조를 제공할 의무를 할당하고 있다. 이는 보안통관에 필요한 수출입 당사자 간 상호 협력과 지원을 보장함으로써 수출입 물류 프로세스를 개선하고 수출입 계약의 이행과정에 수반되는 보안통관절차에 관한 매매당사자간 책임 및 비용의 소재를 명확히 하는데 도움이 된다.

Incoterms® 2010에 규정된 매도인과 매수인의 보안관련 의무는 현재 도입·시행 중인 다양한 물류보안 프로그램에 따라 발생하는 것인 만큼, 그 의의 및 적용범위, 그리고 당해 의무의 이행에 따른 위험 및 비용의 분담관계는 수출입 계약의 이행과정에 수반되는 물류보안 프로그램과 관련하여 살펴볼 필요가 있다. 이에 본 논문은 물류보안제도의 발전과정과 핵심쟁점들을 정리하고,

현재 시행 중인 물류보안 프로그램의 요건상 Incoterms® 2010 규칙에 따라 매매당사자가 부담해야 할 보안관련 의무를 분석한 후 Incoterms® 2010 규칙상 보안관련 의무 규정의 신설이 수출입 거래관계에 미칠 영향을 시사점으로 제시함을 목적으로 한다.

이와 관련한 선행연구로는 세관의 사전전자정보 제출과 Incoterms® 2010의 보안관련 정보제공 규정과의 관계를 다룬 송선욱 교수의 논문이 유일하다. 이 논문은 Incoterms® 2010상 보안관련 정보제공의무가 24hour Rules 등 세관의 사전전자정보 제출규정과 관련하여 수출자에게 미칠 영향을 분석한 것으로 주로 수출자의 보안관련 정보제공의무에 초점을 맞추고 있다. 본 논문은 이를 더욱 확장하여 Incoterms® 2010 규칙상 보안관련 의무의 의미를 분석하고 사전전자정보 제출규정을 비롯한 컨테이너화물 검색제도나 물류보안 인증제도 등 다양한 물류보안프로그램과 관련하여 매도인과 매수인이 부담해야 할 위험 및 비용의 분담관계를 구체적으로 검토하고자 한다.

Ⅱ. 물류보안제도의 발전과 주요 내용

1. 무역패러다임의 변화

1) 무역원활화와 수출입 물류보안

세계관세기구(WCO)는 신속한 세관통과로 무역량을 증가시킴과 동시에 높은 수준의 관리와 검사를 통한 효율적인 세관업무를 위해 세관검사의 질을 향상시키는 동시에 국제적으로 통일화된 방법으로 불필요한 무역제한요소를 제거하고자 노력해 왔다. 그 결과 '73년 『세관절차의간소화 및 조화에 관한 국제협약, 일명 교토협약』(International Convention on the Simplification and Harmonization of Customs Procedures)을, '99년에는 개정교토협약[2](Revised Kyoto Convention of 1999)을 채택해 효과적으로 세관 관리를 달성할 수 있

2) 세관절차의 간소화 및 조화에 관한 국제협약 개정의정서가 정식 명칭인 개정 교토협약은 세관절차의 단순화와 조화를 통해 무역확대에 기여할 목적으로 1973년 교토총회에서 채택된 협약을 1999년 개정한 것으로 2006년 2월 발효되었다.

는 간소하고, 효율적이고, 예측 가능한 세관절차의 마련을 위한 통일된 원칙을 제시했다.

2001년 9월 11일 미국에서 발생한 테러공격은 무역의 촉진보다는 국경에서 물자의 이동에 따른 제약을 강화하는 계기가 되었다. 국제공급망의 보안이 보다 중요한 과제로 등장하면서 세관의 역할이 무역 원활화에서 보안 및 국경보호로 선회하게 된 것이다. 이러한 글로벌 물류환경변화 추세에 대응하여 WCO는 9·11 테러 이후 세관환경 보안의 필요성을 반영한 통합 공급망 관리지침[3]을 마련하였고, 이후 2005년 국제무역의 안전과 원활화를 위한 표준틀(SAFE Framework)을 제정하였다. SAFE Framework는 기존 개정교토협약의 무역 원활화 원칙을 강조하는 한편, 9·11 테러 이후 세관환경 보완의 필요성을 반영한 통합 공급망 관리지침을 근거로 하고 있다. 즉 이는 세관과의 네트워크 및 세관과 기업 간 파트너십 구축을 통해 국제공급망의 보안강화 및 무역원활화를 동시에 추구하는 목표를 가지고 있다.

2) 세관 국경관리 패러다임의 변화

SAFE Framework의 채택에 따른 세관행정의 변화는 다음과 같이 4가지로 요약할 수 있다.[4]

첫째, 과거에는 세관에서 수출입 통관업무를 처리함에 있어서 절차의 신속성에 중점을 두어 왔으나 9.11 테러사태 이후 신속뿐만 아니라 안전에 주안점을 두고 수출입 신고의 정확성을 지향하고 있다. 둘째, 과거에는 수출입 업무와 관련하여 물품을 기준으로 위험도를 분석하고 관리하였으나 AEO 제도가 도입된 이후에는 기업 또는 사람의 신뢰도와 안전도를 중심으로 위험관리를 하고 있다. 셋째, 과거에는 국내 기업과 국내로 수입되는 화물의 관리에 중점을 두었으나 9.11 테러 이후 국제적인 협력을 강화하여 수출국가에서 선적되기 전 안전성을 검사하는 등 세관영역을 국외로 확장하여 수출입 공급망의 안

---

3) 2002년 6월 WCO에서 채택한 통합 공급망 관리지침은 세관 및 기업 전문가들로 이루어진 특별위원회 구성, 개정 교토협약 및 이행지침을 토대로 통합 공급망 관리(ISCM)에 대한 지침을 마련하였고, 향후 AEO 제도의 기반이 된 안전한 경제운영인(Secure Economic Operator), 공인무역업자(Authorized Trader), 공인 수출입 공급망(Authorized Supply Chain) 등의 개념에 대한 정의를 포함하고 있다.

4) 관세청, AEO 가이드북, 2009, p. 10

전을 도모하고 있다. 넷째, 과거에는 특정 시점·장소에서 단편적으로 관리하였으나 AEO 제도에서는 수출입 공급망 전체의 안전에 중점을 두는 흐름 중심의 통합관리를 지향하고 있다.

한편, WCO에서는 세관 공급망 보안 패러다임(CSCSP: Customs Supply Chain Security Paradigm)을 사전 화물정보제공 요건의 확장, 보안관련 위험관리수단의 강화, 컨테이너 화물 검색을 위한 비파괴검사장비 등 첨단기술의 활용, 그리고 보안요건의 준수와 인증된 거래자에 혜택을 부여하는 소위 AEO 프로그램의 도입 등 4가지로 요약하고 있다.[5)]

2. 물류보안제도의 발전과정

Jim Giermanski 박사[6)]는 공급망 보안의 발전을 3단계로 구분하고 있다. 제1단계는 9.11 테러 이전의 무역원활화를 위한 세관행정의 조화를 꾀하는 단계로, 1999년 개정교토협약을 그 바탕으로 하고 있다. 개정교토협약에 따른 관세행정모델은 세관과 무역업계의 협력관계에 기초한 관세행정의 효율적인 운영에 초점을 두고 있다.

제2단계는 9.11 테러 이후 잠재적인 공급망의 위협에 대응하여 미국을 중심으로 진행된 보안프로그램의 도입으로 주로 해운항만분야에 중점을 두고 추진되었다. 이 시기에 도입된 대표적인 보안프로그램은 미국에서 도입한 반테러 민관협력프로그램(C-TPAT, 2001)과 컨테이너 보안협정(CSI, 2002), 미국의 해운보안법(MTSA: Maritime Transport Security Act, 2002), IMO의 국제선박 및 항만시설 보안규약(ISPS Code, 2004) 등이다.

제3단계는 보안의 문제가 공급망의 전반으로 확대되는 단계이다. WCO는 2005년 『SAFE Framework』를 채택하고 무역안전과 원활화를 조화시키는 표준협력으로 AEO(Authorized Economic Operator)제도를 도입하였다. 미국의 C-TPAT 프로그램은 2005년에서 2007년에 걸쳐 화물의 적입단계에서부터 최종 목적지에 이르기까지 수입업자와 운송인이 준수해야 할 새로운 보안요건

---

5) Robert Ireland, The Customs Supply Chain Security Paradigm and 9/11: Ten Years On and Beyond, *WCO Research Paper No. 18*, Sep. 2011, pp. 3-9.

6) Jim Giermanski, The Development and Globalization of Container Security, *Defence Transportation Journal*, September 2008, pp. 16-22

을 추가하였다. 미국은 2006년 미국의 세관 및 국경보호국(CBP)에서 자발적 차원에서 시행해왔던 C-TPAT와 CSI를 입법화하고 9.11 테러 이후 지금까지 미국이 견지해온 대량살상무기(WMD: Weapons of Mass Destruction)의 차단과 테러방지를 위한 모든 조치를 망라한 SAFE Port Act를 통과시켰다. 또한 2007년에는 화물의 발생지에서 도착지까지 트럭, 철도, 선박에 대한 보안을 요구하는 9/11 테러대책위원회 권고이행법률(The Implementation Recommendations of the 9/11 Commission Act of 2007)을 통과시켰다.

3. 물류보안제도의 유형

9·11 테러 이후 미국을 중심으로 시행되기 시작한 이 같은 테러 예방 및 물류보안제도는 양자 및 다자기구로 확산되면서 개별 국가 위주에서 글로벌 기준으로 정착되고 있다. 국제해사기구(IMO), 국제노동기구(ILO), 그리고 경제개발협력기구(OECD) 등 국제기구는 미국과 유사한 제도를 도입하여 전 세계적으로 동일한 기준에 따라 물류보안을 더욱 확대하고 있다.

미국과 국제기구를 중심으로 도입되고 있는 물류보안제도는 적용범위에 따라 선박과 항만 등 특정구간을 적용대상으로 하고 있는 제도와 물자의 발생지에서 최종 소비지에 이르는 공급사슬의 전 구간을 적용 대상으로 하고 있는 제도로 대별할 수 있다. 물류보안제도는 항만이나 선박을 중심으로 이루어지던 초기 단계에서 벗어나 공급사슬 전 구간으로 적용범위를 확대하고 있다.

한편, 물류보안규정의 강행성 여부에 따라 미국의 해운보안법(MTSA) 및 항만보안법(SAFE Port Act)에 기초한 컨테이너화물 검색제도, 국제해사기구(IMO)의 국제선박 및 항만시설 보안규정(ISPS Code) 등 강행적 규제와 CSI나 C-TPAT, AEO 등 참여당사자에게 경쟁적인 이점을 제공함으로써 물류보안을 강화하는 한편, 물자의 이동을 촉진하기 위한 물류보안 인증프로그램들이 있다.

4. 물류보안프로그램의 주요내용

현재 국제적으로 도입·시행되고 있는 물류보안프로그램은 선박 및 항만보안제도, 컨테이너화물 검색제도, 물류보안 인증제도로 구분할 수 있으며, 이들

프로그램의 주요 특징은 위험관리체계의 구축, 사전 화물정보의 제공, 화물 선별검사 및 물류보안인증에 따른 인센티브의 제공 등으로 요약할 수 있다.

1) 선박 및 항만 보안제도

① 미국 해운보안법(MTSA: Maritime Transport Security Act, 2002)

2002년 말 제정된 해운보안법은 미국 해역을 운항하는 선박과 항만시설에 대한 보안조치를 강화하는 규정과 함께 외국항만에서 시행하고 있는 보안제도의 적정성을 평가하는 내용까지 포함하고 있다. 그 밖에 해운보안사고에 대한 대응계획의 수립과 보안지역으로 지정된 곳의 출입을 통제하는 운송보안카드제도의 도입, 선박자동식별장치(AIS: Automatic Identification System)의 설치를 의무화하고 있을 뿐만 아니라 위성통신기술이나 조난선박 구조 및 해상안전시스템(GMDSS: Global Marine Distress and Safety System)을 이용한 광대역 선박위치추적시스템을 개발하고, 입항선박에 대해 적재하고 있는 화물의 정보를 사전에 신고하도록 규정하고 있다.

미국 해운보안법은 국토안보부 장관에게 미국으로 향하는 선박이 출항하는 외국항만이 시행하고 있는 반테러조치의 실효성을 판단하여 적절한 조치를 취할 것을 명시하고 있는 바, 외국항만에 대한 보안평가결과 당해 항만이 적절한 조치를 강구하고 있지 못한 것으로 판단되는 경우 적절한 개선대책을 마련할 것을 해당 국가에 권고할 수 있으며 미국의 입항을 통제하는 조치를 내릴 수 있다.

② 미국 항만보안법(SAFE Port Act, 2006)

미국 국토안보부(DHS: Department of Homeland Security)는 현재 시행하고 있는 제도만으로는 대량살상무기를 효과적으로 차단하는데 한계가 있다고 판단하고 법적 토대를 마련하기 위해 2006년 10월 13일 항만보안법(SAFE Port Act)을 공포하였다. 이에 따라 미국은 2002년에 제정된 해운보안법과 함께 해운 및 항만 분야에 걸쳐 거의 완벽한 보안 시스템을 갖추게 됐다. 항만보안법은 ① 국내의 항만에 첨단기술을 이용한 방사능탐지장치의 설치, ② 항만시설의 운영 · 경비의 강화, ③ CSI 및 C-TPAT의 법제화, ④ DHS에 국내 핵 탐지국(Domestic Nuclear Detective Office)을 설치하고, 방사능물질의 반입방지, ⑤ 항만이 테러공격을 받은 경우의 신속한 사후처리대책의 구축, ⑥

휴대전화 서비스를 이용한 경보시스템의 설치 등을 실시하는 권한을 규정하고 있다.[7]

항만보안법의 가장 큰 특징은 미국이 지금까지 취해온 대량살상무기 차단과 테러예방 등 거의 모든 조치가 망라되어 있다는 점이다. 항만보안법이 시행되면, 미국으로 수출되는 화물에는 컨테이너 보안장치(CSD: Container Security Device) 또는 전자봉인(e-Seal) 등 화물에 대한 상세정보를 담은 보안장치가 부착돼야 한다.[8] 보안장치가 부착되지 않은 수출화물에 대해선 검색 등 통관 절차를 모두 거쳐야 하기 때문에 상대적으로 불이익을 받을 수밖에 없다.

③ 국제해사기구의 선박 및 항만설비 보안을 위한 국제규약

국제해사기구(IMO)에서도 해운산업에 대한 테러방지대책의 필요성을 점차로 인식하게 됨에 따라 해운산업에 대한 테러행위를 예방하고 퇴치함은 물론 해상에서 보안을 강화하기 위한 일련의 규정들이 2002년 12월 국제해사본부에서 개최되었던 외교회의에서 채택되었으며, 2004년 7월 1일 발효하였다. 선박 및 항만설비 보안을 위한 국제규약(ISPS Code: International Code for the Security of Ships and of Port Facilities)은 동 외교회의에서 채택된 1974년 국제해상인명안전협약[9](SOLAS: International Convention on the Safety of Life at Sea)에 대한 다수의 개정안의 일부(Ch. XI-2 해상안전의 강화를 위한 특별조치: 신설)로 국제무역에 사용되는 선박 및 항만설비에 영향을 미치는 보안위협을 탐지하고 제거하기 위한 제도적 장치이다. SOLAS협약 제XI-2장은 해상보안에 관한 세부 이행사항에 대하여 ISPS Code에 위임하고 있으며, 동 규칙은 강제사항인 A편과, A편의 규정들을 준수하기 위한 권고지침인 B편으로 구성되어 있다.

ISPS Code는 국제무역에 사용되는 선박 및 항만설비에 영향을 미치는 보안

---

7) 한상현 · 최준호, WCO 표준(Standards)에 대응하기 위한 각국의 보안조치 강화 방안, 관세학회지 제8권 제4호, 2007, pp. 84-85.

8) 항만보안법에서는 2008년 10월 15일까지 외국으로 운송되는 모든 컨테이너는 국제표준기구 (ISO)의 봉인기준(ISO/PAS 17712)에 따르도록 하고 있다.

9) 1914 년 협약을 시초로 시대의 변천이나 기술의 진보와 함께 1929, 1948, 1960, 1974 년 순차적으로 개정되었다. 74/78 SOLAS 협약은 해상에서 인명안전을 목표로 선박 항행에 관한 통일된 규칙, 복원성, 기기, 전기설비, 방화설비 및 선박구조 등을 규정하고 있다.

위협을 탐지하고 제거하기 위한 제도적 장치로 선박회사는 회사보안책임자[10](CSO: Company Security Officer)와 선박보안담당관[11](SSO: Ship Security Officer)을 임명해야 한다. 선박은 자체보안계획을 수립하고, 기국정부의 보안심사를 받은 후 국제선박보안증서(International Ship Security Certificate: ISSC)를 비치 운항하여야 한다. 항만시설당국은 항만시설보안책임자(PFSO: Port Facility Security Officer)를 임명하고 항만보안평가를 실시 한 후 보안계획을 수립하여 당해 정부의 승인을 받아야 한다. 각 국의 정부는 자국의 선박, 항만의 보안계획승인, 보안심사와 자국항만에 입항하는 외국선박에 대하여 항만국통제[12](PSC: Port State Control)를 실시하여 ISPS Code의 준수유무, 즉 보안상태를 점검하고 위험선박에 대해서 입항금지, 억류, 항만 내에서 이동을 포함한 운행의 제한, 추방 등의 조치가 가능하며, IMO에 자국의 보안관련 사항을 보고해야 한다.

2) 컨테이너 화물 검색제도

컨테이너는 밀수, 불법이민, 대량살상무기의 밀반입 등에 이용될 가능성이 높고, 컨테이너 선박은 그 자체로서 테러공격의 타깃이 되거나 테러공격을 위한 무기나 수단으로 이용될 수 있으며, 선박의 등록 및 소유관계에 있어서 투명성의 결여는 테러분자들이 선박을 범죄적인 목적에 악용할 수 있는 소지를 제공한다는 점에서 보안위험을 초래할 가능성이 높다.[13] 컨테이너 화물검색제

---

10) 항만시설보안책임자 및 선박보안담당관과의 연락을 위하여, 그리고 선박보안계획을 개발하여 승인을 위한 제출, 시행 및 유지를 위하여 회사가 지정한 자를 말한다.

11) 회사보안책임자 및 항만시설 보안책임자와의 연락을 위하여, 그리고 선박보안계획서의 시행과 유지를 포함하여 선박의 보안책임자로 회사가 지정한 선장에 상응하는 자를 말한다.

12) 항만국이 자국의 관할해역에서 해상안전을 도모하고 해양환경을 보호하기 위하여 자국 항구에 기항하는 외국 국적의 선박을 대상으로 국제협약상 기준에 따라 선박의 안전기준, 선원의 자격, 근로조건 및 선원의 운항능력 등을 점검하고 '기준미달'로 판명되거나 또는 오염물질 배출규정을 위반한 경우 입출항을 규제하고 국제기구에 당해 선박의 결함정보를 보고하는 등 불이익한 처분을 행사하는 제반 행위를 말한다.

13) 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)

도는 선적 전 검사 및 위험도가 높은 컨테이너 화물에 대한 사전 정보입수 등을 통해 컨테이너가 테러행위에 악용될 소지를 줄이고 대량살상무기 등이 컨테이너를 통해 밀반입되는 것을 차단하기 위한 조치이다.

시행 중인 컨테이너 화물 검색제도

시기	내 용	관련 법령
2002. 1	CSI(Container Security Initiative)	SAFE Port Act(2006. 10)
2003. 2	24 Hour Advance Vessel Manifest Rule	SAFE Port Act(2006. 10)
2007. 3	SFI(Security Freight Initiative)	SAFE Port Act(2006. 10)
2009. 1	ISF(Importers Security Filling)	SAFE Port Act(2006. 10)
2011. 1	EU-ICS(Import Control System)	EC Regulation 648/2005, 1875/2006
2012. 7	SFI(Security Freight Initiative)	9.11 테러대책위원회 권고이행법(2007. 8)

① 컨테이너 보안협정 (CSI: Container Security Initiative)

컨테이너보안협정은 국제 테러조직들이 대량살상무기 등을 밀반입 하는 것을 차단하고 무역공급망을 마비시키기 위해 수송 도중의 컨테이너를 폭파시킬 가능성에 대비하기 위해 미국 관세 및 국경보호국(CBP: Customs and Border Protection)에서 도입한 세관 간 협력프로그램이다. 이 제도의 핵심은 외국 항만에서 현지국 세관원이 미국 세관원과 공동으로 미국행 컨테이너 화물의 선적 24시간 전에 화물투시기(X-ray)나 방사능 탐지기 등으로 위험화물을 사전 검색·적발하여 미국 입항을 금지하는 등 적절한 조치를 취하는 것이다.[14]

CBP의 주도 하에 미국과 개별 국가 간의 양자협정을 체결하여 이루어지던 이 제도는 2006년 항만보안법(SAFE Port Act)이 통과되면서 법제화 되었고, 화물의 검색비율을 100%로 높이는 시범사업을 진행하도록 규정하게 되었다.

14) 미국은 컨테이너보안협정의 적용대상으로 미국행 화물을 대량으로 선적하는 세계 20대 항만(mega port)을 우선 선정하였고, 제도 도입 초기인 2003년 대상항만 거의 대부분이 이 제도를 시행하기로 미국과 양자협정을 체결하였거나 시행한다는 원칙에 합의하였다. 미국으로 반입되는 컨테이너 화물 중 약 68%가 20대 주요 항만으로부터 반입되고, 반입되는 해상 컨테이너 중 약 86%가 CSI 항으로부터 반입되고 있다. 유럽에서는 독일, 네덜란드, 프랑스, 영국 등이 이에 포함되어 있고, 아시아권에서는 중국, 일본, 싱가포르, 홍콩, 우리나라 등이 참여하고 있다. 우리나라는 2003년 1월 미국과 CSI 협정을 체결하였다.

② '컨테이너 100% 검색 시범사업(SFI : Security Freight Initiative)'

미국은 CSI 제도 도입 이후 2006년 항만보안법을 제정하여, 컨테이너 화물 검색제도의 집행을 위한 법적 토대를 마련하였다. 동 법률에서는 향후 컨테이너화물의 검색비율을 100%로 높이는 시범사업(Pilot Project)을 진행하도록 규정하고 있다. 미국 국토안보부는 2007년 12월에 '컨테이너 100% 검색 시범사업(SFI : Security Freight Initiative)'에 착수하였다. 우리나라 관세청은 2008년 4월 SFI 협약을 맺고 핵 및 방사능 물질에 대한 검색이 가능한 화물영상검색기를 부산 감만부두 허치슨 터미널에 시범설치하기로 하였다.

SFI 프로그램 대상항만

항만명(국가)	운영사	물동량(2006)	계획시기
카심항(파키스탄)	DP World	2,058	2007. 3
푸에르토 코르테스항(온두라스)	Empresa Nacional Portuaria	77,707	2007. 4
사우스햄튼항(영국)	DP World	31,780	2007. 8
부산항(한국)	Hutchison	610,061	2008. 4
살라라항(오만)	APM	81,333	2008. 5
싱가포르항(싱가포르)	PSA	376,846	2008. 6
홍콩항(홍콩)	Modern Terminal	1,333,812	2007. 11

출처: 박찬석, 국제물류보안동향과 시사점, 2008

한편, 2007년 제정된 9/11 테러대책위원회 권고이행법률(The Implementation Recommendations of the 9/11 Commission Act)은 시범사업 단계를 넘어 2012년 7월부터 미국으로 선박을 통해 수출되는 모든 컨테이너 화물에 대해 100% 사전검색을 의무화하고 있다. 즉, 동 법률은 제1701조에서 "외국항만에서 적재된 모든 컨테이너는 직접 또는 외국항만을 거친 것을 불문하고, 선박에 선적되기 전에 비파괴영상장비와 방사능탐지기로 검색(scan)하지 않는 경우 미국에 반입하는 것을 금지한다."고 명시하고 있다.[15] 이에 따라 2012년 7월부터 미국으로 수출되는 화물은 100% 선적항에서 사전 X레이 및 방사능검사 등 사전검색

15) 최재선, 컨테이너화물 100% 사전검색 의무화와 정책시사점, KMI 해양수산 현안분석, 2007-14, pp., 4-7

이 의무화된다.

③ 24시간 전 적하목록 제출제도(24-Hour Advance Vessel Manifest Rule)

CSI의 효과적인 수행을 위한 후속조치의 일환으로 제정된 것으로 운송인이 선적항에서 선적 24시간 전에 미국 세관에 사전 화물적하목록을 제출하도록 규정한 미국 관세청 규칙이다. 미국행 수입화물의 적하목록을 선적 전에 자동적하목록시스템(AMS: Automated Manifest System)에 신고하도록 함으로써 위험도가 높은 화물과 여행자를 선별하기 위한 충분한 시간을 확보하려는 것이다. 또한 외국항만에 파견되어 있는 미국 세관원에게 검사대상 화물에 대한 정보를 즉시 제공하는 효과 외에 외국항만에서 시행된 컨테이너 보안 검사에서 적발되지 않은 미국행 화물을 미국 항만에서 다시 검사할 수 있는 이중 검색 수단으로 활용하려는데 제도의 목적이 있다. 미국은 이와 함께 동 제도를 항공·트럭·철도 수출입화물에까지 확대한 적하목록정보의 전자적 방식에 의한 제출제도(Advance Electronic Cargo Information System -Trade Act of 2002)도 시행하고 있다.[16)]

선사는 화물을 선적하기 24시간 전에 화물정보를 미국 세관에 신고해야 하며, 이때 미국항만에 양륙하지 않는 화물정보도 동시에 신고해야 한다. 이에 따라 한국의 관세청은 미국행 해상화물에 대하여 선사가 화물을 선박에 적재하기 전에 당해선박에 적재할 적하목록을 적재 24시간 전까지 미국 세관과 한국세관에 제출하도록 하는 '적재 전 신고제도'를 시행하고 있다. 이를 위해 화주는 선적 72시간 전에 화물정보를 선사에 제공해야 하며 출발 24시간 전에 해당 화물을 항만에 반입해야 한다.

미국 24 Hour Rule의 주요 내용

16) 김창봉·천홍욱, AEO제도 구축과 물류공급체인망 성과에 관한 연구, 유통경영학회지, 제13권 제1호, 2010, p. 113.

구 분		주요 내용
화주의 의무		• 선사에게 정확한 선적 화물정보(15개 항목) 제공
선사의 의무		• 화물 선적 24시간 전 화물정보 미 관세청에 신고 • 미국항만에 양륙하지 않는 화물정보도 동시 신고
위반 시 처벌규정		• 당해 화물의 미국항만 양륙 허가 불허 • 처음 위반 시 5,000달러 벌금(위반건수 당) • 그 이후의 위반 시 1만 달러의 벌금과 선박 억류 또는 몰수
선화주 대책	화주	• 선적 72시간 전 화물정보 선사 제공 • 출항 24시간 전 해당화물 항만 반입
	선사	• 화물선적 24시간 전에 미 관세청에 신고 • 선적마감시간 고려 화물 선적계획 작성
신고 시 유의사항		화물정보 기재 명확화 – "FAK", "Consolidated Cargo", "Said to Contain" 등 표현 사용 금지 – "26 Pallet" 등과 같이 부정확한 수량표현 금지

출처: 정석물류통상연구원, 한국 수출업체의 물류보안 인식 및 리스크관리 방안, 2008-1

④ 수입자 보안신고프로그램(ISF: Importers Security Filling or 10+2 규칙)

해상으로 수입되는 컨테이너화물의 보안검사와 관련된 기존 24시간 규칙을 강화하기 위한 조치로 항만보안법에 의해 법제화 되었다. 2009년 1월 26일부터 미국의 모든 수입자들은 적재 24시간 전에 10가지, 운송인은 2가지 데이터 항목을 자동적하목록시스템(AMS)을 통해 추가적으로 제출하여야 한다. 이 제도는 미국으로 수입되는 화물뿐만 아니라 미국 이외의 항에서 하역하기 위하여 선박에 적재되어 있는 통과화물이나 환적화물에도 적용된다.

만일 화물에 대한 기술이나 수하인의 성명·주소 기재에 관한 중대한 위반사항이 있는 경우에는 선적불가(Do Not Load) 명령이 내려질 수 있으며 운송인이 정확한 적하목록 정보를 정해진 시간 내에 제출하지 못하거나 허위정보를 제출한 때에는 법에 따라 벌금(건당 미화 $5,000)을 부과하고 선박 전체화물 또는 해당 화물에 대해 화물정보 제출 시까지 양륙허가를 지연시킬 수 있다는 점을 감안할 때 미국의 수입자들은 새로운 보안신고요건과 관련하여 해외 공급업자와 상호 협력하여 적시에 정확한 정보를 제공할 수 있는 방법들을 개발하여야 한다.

10+2 규칙의 내용

전송주체	제출정보	전송시점
수입화주	판매자	선적 24시간 전
	구매자	
	수입자번호(Importer of record number)	
	수하인번호(Consignee number)	
	제조자 또는 공급자	선적 24시간 전 완전한 정보 미확보 시 미국 항 도착 24시간 전까지
	수취인(Ship to party)	
	원산지	
	품목분류번호 6자리(HTSUS)	
	컨테이너 적입장소	미국항 도착 24시간 전
	혼재인(Consolidator)	
선사	화물 적재계획	출항 후 48시간 이내 항해시간이 48시간 이내이면 도착 전까지
	컨테이너 상태메시지	선적 24시간 전

출처: 박찬석, 국제물류보안동향과 시사점, 2008

⑤ EU-ICS(Import Control System)

미국의 10+2 Rule과 유사하게 ICS 역시 선적화물이 EU 역내에 도착하기 전 세관에 주요 선적정보를 전송하여 위험을 평가할 수 있도록 하는 것을 목적으로 하고 있다.[17] ICS 제도는 유럽 의회 및 이사회규정 Regulation No. 648/2005 및 No. 1875/2006에 포함되어 있다. 동 제도는 2009년 7월 1일 처음 도입되었으나 2010년 12월 31일까지 과도기간을 거친 후 2011년 1월 1일부로 강행적으로 시행하고 있다.[18] 즉, 운송인은 EU 영내도착 및 통과화물에 대해 선적화물에 대한 사전 정보를 전자적인 방법으로 EU 세관당국에 제

17) 미국의 ISF 제도는 해상운송화물에 대해서만 적용되는 반면, EU의 ICS 프로그램은 모든 운송화물에 대해 적용된다는 점에서 차이가 있다.(Suzanne Richer, Balancing Global Priorities, *Logistics Management,* January 2011, p. 43)

18) 2009년 7월 EU 회원국 중 체코가 가장 먼저 화물정보 사전 신고제도를 도입하였고 뒤를 이어 2010년 1월 네덜란드가 시행하였다. 적하목록정보를 제출시한 내에 제출하지 않거나 허위로 제출하는 경우에는 EU 개별 회원국의 내부규정에 따라 벌금을 부과한다.

출하여야 한다. 구체적으로는 수입화물이 EU 역내에 도착 전 ENS(Entry Summary Declaration)라는 전자적 형태의 신고가 이루어져야 하며, 당해 신고에 포함되어야 할 사항 및 운송수단별 ENS 신고 시기는 다음과 같다.

EU ICS의 주요 내용

신고사항	운송방법	ENS 신고 시기
• 화물확인을 위한 세부사항 – 수하물고유번호(UCR) – 컨테이너번호, 봉인번호 – 화물명세, 화인 및 상품코드 • 거래 당사자에 관한 사항 – 송하인, 수하인, 운송인, ENS 신고자 등 • 수하인의 신원확인정보와 AEO status • 반입, 통과, 반출 등 구체적인 화물의 이동경로	해상컨테이너화물	선적 24시간 전
	해상 개품화물 및 살화물	EU 역내 도착 4시간 전
	단거리 해상운송(24시간 미만)	EU 역내 도착 2시간 전
	단거리 항공운송(4시간 미만)	이륙시점
	장거리 항공운송(4시간 이상)	EU 역내 도착 4시간 전
	철도 및 내수로 운송	EU 역내 도착 2시간 전
	공로운송	EU 역내 도착 1시간 전

출처: David Merritt (May, 2010)

3) 물류보안 인증제도

물류보안인증제도는 미국이 2002년 4월부터 대테러 민·관 협력제도(C-TPAT)를 시행한 이후 세계세관기구와 국제표준화기구 등도 유사한 제도를 마련하였으며, EU도 WCO의 제도를 수용한 기업 물류보안 인증제도(AEO)를 2008년부터 본격적으로 시행하고 있다. 그 밖에 스웨덴(Stairsec), 뉴질랜드(SES: Secure Export Scheme), 캐나다(PIP: Partner In Protection), 싱가포르(STP: Secure Trade Partnership Program) 등에서도 물류보안 인증제도를 시행하고 있다. 물류보안 인증제도는 세부내용은 다소 차이가 있지만 세관이 무역업체, 물류업체, 관세사 등 민간부문이 준수해야 하는 최소한의 보안기준을 제시하고, 이를 충족한 당사자에게는 특정 자격을 부여(인증)한 후 세관절차의 간소화 및 무역원활화를 위한 인센티브를 제공하는 한편, 인증 받지 못한 업체에 대해서는 집중적인 관리를 함으로써 공급망상의 보안 및 안전을 극대화 하는 것을 핵심적인 내용으로 하고 있다.

① WCO의 SAFE Framework와 AEO제도

세계관세기구는 2005년 6월 무역안전 및 원활화에 관한 표준 틀(WCO SAFE Framework of Standards to secure and facilitate global trade)을 채택하고 무역안전과 원활화를 조화시키는 표준협력으로 AEO(Authorized Economic Operator)제도를 도입하였다. AEO는 9.11 테러사태 이후 강화된 미국의 무역안전조치를 WCO 차원에서 수용하면서 무역안전과 원활화를 조화시키는 과정에서 탄생한 것으로 화주, 선사, 운송인, 창고업자, 관세사 등 화물이동과 관련된 물류주체들 중 각국 세관당국에 의해 신뢰성과 안전성을 공인받은 업체를 의미한다. 현재 EU에서 실시하는 민·관 협력제도의 명칭이기도 한 'AEO'는 전 세계 각 국 관세당국이 실시하는 유사한 민·관 협력제도를 일컫는 대명사가 되었다. 우리나라도 2007년 12월 31일 관세법을 개정해 제255조의 2(수출입안전관리 우수공인업체)를 신설했으며, 2009년부터 '종합인증우수업체'제도[19]를 시행하고 있다.

AEO 제도는 국가 간 상호인정 절차를 갖고 있으므로 우리나라에서 공인된 AEO 기업의 신뢰성과 안전성이 국제적으로 추인되어 우리나라에서 수출하는 AEO 기업은 상대국 수입절차에서 특례를 적용받을 수 있으며 AEO 인증을 받은 기업이 거래업체에 대해 AEO 인증을 받을 것을 요구하는 추세에 비춰 거래선 확보와 유지 등 수출기업의 경쟁력 향상에 기여하게 된다.

② ISO의 물류보안경영시스템 인증제도(ISO 28000)

국제표준화기구도 기업의 보안관리 표준의 필요성에 부응하여 2005년 11월 ISO/PAS 28000 협약을 발표하고 물류보안경영 표준 및 인증제도를 도입하고 있다. ISO/PAS 28000은 생산자로부터 운송·보관업자 등을 포함하는 공급사슬 내의 모든 기업을 적용대상으로 하고 있는 국제표준규격이다. ISO/PAS 28000에 규정되어 있는 보안관리 시스템이 구축되는 경우 인증기관에서 인증을 받게 되면 해당기업은 일정한 보안자격을 갖춘 것으로 인정된다.

ISO 28000은 수출입 안전관리 역량을 강화시키기 위해서 기업에서 비용을 부담하고 도입하는 민간프로그램으로 그 대상이 국제무역공급망 모든 당사자

19) 2009년 4월 '종합인증우수업에 공인 및 관리업무에 관한 고시'의 제정 및 시행에 따라 종합인증우수업체는 통관절차상의 특례를 비롯한 수출입물품의 검사대상 선별제외, 관세법상 관세 등에 대한 담보제공과 정산을 위한 건별, 월별 사후납부를 위한 신용담보 등의 혜택을 누릴 수 있다.

인 점, 안전관리에 관한 경영시스템을 심사한다는 점 등 AEO와 유사하지만 AEO 제도는 국가기관이 ISO는 민간인증기관이 인증주체이며 따라서 ISO 인증을 받은 업체는 국가 간 상호인정의 대상이 될 수 없고 외국에서 통관상의 혜택을 받을 수 없다.[20]

③ 대테러 민관협력 프로그램(C-TPAT: Customs-Trade Partnership Against Terrorism)

C-TPAT는 미국으로 화물을 수출하는 모든 제조업자, 화주, 선사 등에게 화물의 공급사슬 전반에 걸쳐 보안성을 확보하도록 하는 것으로 관세청이 민간기업과의 협정을 통하여 시행하고 있다. C-TPAT는 무역업계가 CBP와 협력하여 자발적으로 법규 및 보안기준을 준수토록 함으로써 보안을 강화하는 동시에 이와 같은 조치가 적용되는 화물 및 운송수단에 대해서는 무역흐름을 촉진하는 수출입 물류보안 프로그램으로 WCO SAFE Framework의 토대가 되었다.

C-TPAT는 제조업자, 수입자, 운송회사, 관세사, 창고 및 항만터미널 운영자 등 공급망(supply chain)의 모든 당사자가 참여하는 프로그램으로 2002년 4월 도입 되었는데, 이 프로그램에는 공급망 당사자들이 준수해야 하는 최소한의 보안기준을 제시하고 있으며, 이를 준수하는 업체에 대해서는 신속통관, 화물검사비율의 축소 등의 혜택을 제공하는 것으로 기본적으로는 자발적이며 신뢰에 기초한 파트너십 프로그램이다.[21]

④ EU의 AEO 제도

EU는 2005년 역내시장을 보호하고 국제 공급망을 보호하며 개선된 세관절차를 통해서 적법한 무역을 원활하게 지원한다는 목표로 일련의 조치들을 도입하였는데, EU 세관보안프로그램(Customs Security Program : CSF)에 포함

---

20) 관세청, 앞의 책, p. 18

21) C-TPAT 프로그램은 인증등급을 3단계로 구분하여 운영하고 있는데, 등급마다 차등적인 통관혜택을 부여하고 있다. 1단계는 프로그램 참여가 허용된 상태로 화물검사회수가 축소되며, 2단계는 1단계의 혜택 외에 화물의 우선적 검사기회 부여, 마지막으로 3단계는 화물검사 면제 외에 다양한 혜택을 부여받게 된다(고현정, 국제물류보안인증제도 동향 및 시사점에 관한 연구, 한국항만경제학회지 제27집 제2호, 2011, p. 341).

된 이들 조치는 공동체관세규약(Community Customs Code : CCC)을 개정함으로써 구체적으로 도입되었다.

주요 내용을 살펴보면, 첫째, 물품을 수출 또는 수입하는 경우 사전 전자정보를 세관당국에 제공하고(pre-arrival and pre departure declarations), 둘째, EU 회원국을 위한 공동위험선별기준(common risk-selection criteria)에 기초한 공동위험관리기법을 도입하며, 셋째, 적법한 무역을 촉진하기 위해서 신뢰할 수 있거나 세관법규준수도가 뛰어난 무역업자들에게 간소화된 세관절차를 제공하는 것이다. 2008년 1월부터 AEO 제도가 시행중이며, AEO 인증을 위한 보안기준은 기업정보, 법규 및 기준 준수도, 기업의 회계 및 물류시스템, 재정건전성, 안전 및 보안 요구사항 등 5개의 부문으로 구성되어 있다. AEO 인증을 받은 업체들은 세관절차의 간소화, 물리적 화물검사 횟수의 경감, 선적물품에 대한 반출입 우선 처리 등의 혜택을 받고 있다.

Ⅲ. Incoterms® 2010 규칙상 매매당사자의 보안관련 의무 분석

1. Incoterms® 2010 규칙상 보안관련 의무의 의의

Incoterms® 2010 규칙상의 수출입 통관에 관한 주요 원칙들은 기존과 동일하지만, 수출입 매매당사자 간 상호 협조의무가 필수적인 요건이 되었다. 다시 말해 Incoterms® 2010 규칙은 기존의 허가, 인가 및 통관절차에 관한 규정 등을 새롭게 개정한 것이 아니라, 수출입 과정에서 요구되는 화물보안 요건들의 준수를 매도인과 매수인의 강행적인 의무로 규정한 것이다.[22] 따라서

22) 기존의 Incoterms 규칙에서는 화물보안의 문제에 적용될 수 있는 용어를 이미 포함하고 있었다. Incoterms 2000에서는 매도인과 매수인의 의무 A2/B2에서 허가, 인가 및 공적절차(License, Authorization and Formalities)를 규정하고 있다. 여기서 매수인은 물품의 수입에 관한 자신의 의무가 자신의 위험과 비용으로 수입허가 및 공적 인가를 취득하고 적용가능한 경우 수입통관절차를 수행하는 것임을 알 수 있다. A10의 "Other Obligation"에서는 물품의 수입을 위해 매수인이 요구하는 선적지 국가에서 발행되거나 전송되는 모든 서류 혹은 그에 상응하는 전자적 메시지를 취득하는데 있어서 매수인에게 모든 협조를 제공할 매도인의 의무를 규정한다. Incoterms 2000상의 이들 규정들은 화물보안과 관련한 의무의 부담을 할당하는 근거가 된다. 여기에 Incoterms 2010 규칙에서는 통관절차(customs formalities)와 보안관련 기능(security-related function)을 구분하는 용어를 추가하였다.

매도인과 매수인은 Incoterms® 2010 규칙 A2/B2, A10/B10의 규정에 따라 보안통관을 이행하기 위해 요구되는 정보 및 필요한 지원을 제공해야 할 의무를 부담하게 되었다. 물류보안프로그램의 준수를 위한 수출입 당사자 간의 협력(collaboration)은 기존의 규칙에서 다루어지지 않았던 것으로 Incoterms® 2010 규칙에서 매매계약 당사자에게 새롭게 요구되는 의무이다.[23]

1) 보안통관 및 그에 요구되는 정보

Incoterms® 2010 서두(introduction)에서는 최근 물자의 이동에 있어서 보안에 대한 우려가 증가함에 따라 물품이 그 고유한 성질 이외의 다른 이유로 생명이나 재산에 위협이 되지 않음을 확인하도록 요구하고 있는 바, Incoterms® 2010 개별 규칙의 A2/B2, A10/B10에서 매도인과 매수인 간에 보관의 연속성에 관한 정보(chain of custody information)와 같이 보안통관(security-related clearance)을 완료하거나 그에 필요한 지원을 제공할 의무를 할당하고 있음을 밝히고 있다.[24]

제Ⅱ장에서 검토한 바와 같이 국제적으로 도입·시행중인 물류보안제도는 국제협약이나 일국의 국내법에 따라 강행적인 준수의무를 부과하는 제도와 인증을 통해 다양한 인센티브를 제공함으로써 개별 공급망 주체가 자율적으로 물류보안체계를 구축하도록 유도하는 물류보안 인증제도로 나뉜다. 이와 관련하여 Incoterms® 2010 규칙상 보안통관 및 그에 필요한 지원을 제공할 매도인과 매수인의 의무가 물류보안제도상 강행적으로 요구되는 사항에 국한되는 것인지 통관과정상의 다양한 혜택을 제공받기 위한 물류보안인증에 필요한 요건들을 포함하는 것인지 여부가 문제로 된다.

Incoterms® 2010 규칙에서는 이에 관한 명확한 언급이 없지만, WCO의 SAFE Framework를 토대로 현재 45개국 이상이 물류보안 인증제도를 시행

글로벌 공급사슬에서 물류보안의 중요성이 증대되면서 여러 국가에서 입법적으로 이들 두 행위를 구분함에 따라 국제상업회의소에서 이러한 추세를 반영하여 Incoterms 2010 규칙에서 통관 및 보안에 대한 매도인과 매수인의 의무를 모두 규정한 것이다(Dan Gardner, A New Chapter in Incoterms, *The Journal of Commerce*, Sep. 15, 2008, p. 60.).

23) David Lowe, Incoterms 2010: Making trading easier, *Practical Law for Companies,* Vol. 21. Part 9, 2010, p. 11 (pp. 11-13)

24) Incoterms® 2010, International Chamber of Commerce, 2010, p. 9

중이며, 물류보안인증을 받은 업체 수가 지속적으로 증가하고 있음을 감안할 때 거래 파트너의 선정에 있어서 물류보안인증과 관련한 보안의무의 준수를 요구하게 될 것은 분명하다.

〈물류보안인증업체 현황〉

국가	프로그램 명칭	공인업체 수	시행 시기
미국	C-PTAT	9,386	2002
싱가포르	STP	20	2008
뉴질랜드	SES	116	2004
일본	AEO	354	2007
EU	AEO	1,459	2008
중국	CACC	1,140	2008
한국	수출입 안전관리 우수공인제도	181	2009

출처: 관세청 (2010. 7)

또한 Incoterms® 2010 개별규칙 A2/B2와 A10/B10에서는 해당되는 경우, 상대방 당사자의 요청에 따라 상대방 당사자에게 보안통관에 요구되는 정보를 제공하거나 그에 필요한 지원을 제공하도록 규정하고 있다. 이는 매도인이나 매수인은 각 국에서 시행 중인 물류보안프로그램에 따라 보안통관을 위해 강행적으로 요구되는 요건을 충족하기 위해 보안정보를 제공하거나 물류보안인증에 따른 혜택을 제공받기 위해 상대방 당사자가 요청하는 경우 필요한 지원을 제공하여야 하는 것으로 해석할 수 있다.

한편, 물류보안제도는 그 적용범위에 따라 특정 구간에 대해서만 적용되는 경우와 공급사슬 전반에 걸쳐 적용되는 경우로 나뉘는 바, Incoterms® 2010 규칙 A10, B10에서는, 물품의 수출입 및 운송, 제3국을 통과하는 운송, 그리고 최종 목적지로의 운송에 필요한 서류와 정보를 제공하거나 그러한 서류와 정보를 획득하는데 필요한 지원을 제공하도록 규정하고 있는 바[25], 매도인과 매수인은 공급사슬 전반에 걸친 보안의무의 이행이 요구된다고 볼 수 있다.

---

25) ... needs for the export and import of the goods, for the transport and for their transport through any country, for their transport to the final destination...

이러한 견지에서 보안통관(security clearance)은 수출입 물품의 국경 간 이동에 있어서 불필요한 시간이나 비용을 초래하지 않도록 개별 국가 혹은 국제기구에서 공급망 보안을 확보하기 위해 도입·시행 중인 강행적인 물류보안 프로그램의 준수 및 AEO 등 물류보안인증에 필요한 요건 및 절차의 이행을 의미하는 것으로 볼 수 있다.

2) 보관의 연속성에 관한 정보

보관의 연속성(chain of custody)은 증거물이 수집된 후 법정에 제출될 때까지 동일한 상태로 안전하게 보관되어야 한다는 것을 의미하며, 이는 점유(seizure), 보관(custody), 통제(control), 전달(transfer), 분석(analysis), 및 물리적 전자적 증거의 처분(disposition)을 보여주는 문서화된 절차(documented process) 등 증거의 무결성(integrity)을 보증하기 위한 절차적인 방법으로 사용된다. 문서에는 증거수집조건, 당해 증거를 취급한 모든 당사자의 신원확인, 증거보관기관, 증거의 취급 및 보관상의 보안조건, 각각의 경우에 있어서 증거가 후속 관리자에게 전달되어진 방법들이 포함되어야 한다.[26]

공급사슬관리와 관련하여 보관의 연속성이 적절히 유지되기 위해서는 3가지 요건이 필요하다.[27] 첫째, 화물이 본래의 목적 및 서류상에 기재된 수량을 유지하고 있을 것. 둘째, 당해 화물이 발생지에서 컨테이너에 적입될 당시부터 최종 목적지에서 인도될 때까지 운송인의 계속적인 점유 혹은 통제 하에 있었을 것. 셋째, 당해 화물의 이동 과정에 개입한 개별 당사자의 신원에 관한 증거 및 당해 화물이 컨테이너에 적입·봉인된 때로부터 수령인의 관리하에 인도·방면할 때까지 동일한 상태를 유지하고 있음을 입증할 것.

컨테이너 화물의 적입 단계에서 최종 인도에 이르는 전 과정에 걸쳐 관계당사자들은 당해 화물이 자신의 관리(통제)하에 있는 동안 화물의 변조(tampering), 도난 및 손상을 방지하고, 보안심사(security screening)를 위한 정확한 정보를 적시에 정부기관에 제공하는 한편, 화물에 관련된 정보의 변조

---

26) Jim Giermanski, The Impact of Incoterms® 2010 on Supply Chain Security Both Global and Domestic, *The Maritime Executive*, May 11, 2011 http://www.maritime-executive.com)

27) Jim Giermanski, Tracking and Chain of Custody: The Difference, *The Maritime Executive*, November 17, 2011 (http://www.maritime-executive.com)

방지 및 승인되지 않은(unauthorized) 접근을 차단하는 등의 보안의무를 부담한다.[28] 컨테이너 화물의 점유 혹은 관리 주체가 바뀌는 경우에는 이들 당사자들 간의 관계에 있어서 보안을 유지하기 위한 보관의 연속성이 확보되어야 한다.

보관의 연속성을 유지함에 있어서 인적요소는 핵심적인 부분이다. CBP에서 시행하고 있는 C-TPAT의 9가지 핵심 구성요소에도 공급망에서 물자의 흐름에 관여하는 인적보안(personal security)이 포함되어 있다. 글로벌 공급망의 보안에 있어서 보관의 연속성은 화물의 내용 및 수량, 운송용구 및 운송계약상 필요한 기타 모든 사항들을 검증하는 당사자의 신원을 확인하는 것에서부터 시작된다. 적재시점부터 관리 혹은 통제권한의 이전, 접근의 허용 등 매 단계에 개입하는 모든 당사자의 서명 혹은 신원확인도 필요하다.

컨테이너 화물의 보안을 위한 부착되는 봉인(seal)은 보관의 연속성을 유지함에 있어서 중요한 부분을 담당한다. 화물이 적입된 컨테이너의 관리주체가 변경될 때마다 수령인은 컨테이너 봉인의 이상 유무를 점검하여야 한다. 이를 위해서는 우선 변조 징후를 확인하기 위한 시각검사(visual check)를 하고, 선적서류와 봉인 고유번호를 대조한 후 검사결과를 문서로 기록하는 절차가 필요하다. 만일 봉인이 분실되거나 변조의 징후가 보이는 경우, 혹은 봉인번호가 선적서류상의 기록과 다른 경우 일정한 조치가 요구된다.

오늘날 재화의 국제적 이동에 수반되는 컨테이너나 트레일러 등 운송용구는 컨테이너보안장치(CSD: Container Security Device)[29]를 활용하여 공급망 전 과정에 걸쳐 보안을 유지하고 감시함으로써 보관의 연속성을 보장할 수 있다. CSD는 화물의 정확성을 입증할 책임 있는 당사자의 신원을 확인하고 합의된 물류정보가 당해 정보를 필요로 하는 적절한 당사자에게 위성 혹은 무선통신

---

28) WCO, WCO SAFE Framework of standards, June, 2011, p. 21

29) 선박을 통해 수출입되는 컨테이너에 부착하는 안전장치로 RFID와 Magnetic Sensor를 이용하여 Container Door가 불법적 행동에 의해 열리는 상황을 감지하는 일을 하는 물류보안장비이다. 화물 컨테이너의 내부에 장착되며, 컨테이너 화물의 분실, 도난, 컨테이너 위치 추적 및 컨테이너 침입 탐지의 기능을 수행한다. 미국 CBP의 권고사항으로 처음에는 Container Security Device에서 Conveyance Security Device로 개념이 바뀌.어 제조공장으로부터 선적항을 통한 수화주 공장까지의 물류전반의 Traceability를 확보하기 위한 목적으로 사용된다(KEIT, 화물컨테이너용 보안장치 기술동향 및 국제 표준화 이슈, KEIT PD Issue Vol. 10-2, p. 21).

망을 통해 컨테이너로부터 자동으로 전송함으로써 국제운송화물의 내용 및 수량을 전자적으로 검증할 수 있도록 한다. 매도인, 매수인 및 기타 당사자들은 CSD를 통해 화물의 이동과정을 추적하고 운송중인 컨테이너 화물에 대한 정보를 조회할 수 있다. CSD는 목적지에서 컨테이너에 접근하기 위해 필요한 전자적 통신 혹은 생체인식(biometric reading) 등의 방법을 통해 컨테이너 화물의 인도수령 및 컨테이너의 개폐권한을 가진 개인의 신원을 전자적으로 확인함으로써 보관의 연속성 절차를 구현한다.[30]

더욱이 미국의 연방 민사소송법(Federal Rules of Civil Procedure)이 일부 개정됨으로써 CSD를 통해 전자적으로 저장된 정보도 민사소송에서 증거로 사용될 수 있는 여지를 가지게 되었는 바, 수출입 당사자가 C-TPAT나 10+2 Rules와 같은 물류보안프로그램의 강행적인 요건을 준수하였는지 여부와 관련한 분쟁에도 활용될 수 있다.

2. 허가, 인가, 보안통관 및 기타 공적 절차 이행의무

1) 보안통관을 위한 매도인의 정보제공의무 (A2)

Incoterms® 2010 규칙 A2에서는 매도인은 해당되는 경우, 매수인의 요청에 따라 매수인의 위험과 비용부담으로 매도인이 보유하고 있는 물품의 보안통관(security clearance)을 위해 요구되는 정보를 매수인에게 제공하도록 규정하고 있다. 이러한 내용은 Incoterms 2010의 11개 규칙 중 EXW 규칙에만 규정되어 있다. 이는 EXW 규칙상 수출허가 및 기타 공적인가를 취득하는 것이 매수인의 의무로 되어 있는 바, 수출지에서 화물의 보안확인을 위해 매도인의 관련정보제공이 필요하기 때문인 것으로 판단된다.

EXW 규칙 A2에서 보안통관에 요구되는 정보를 제공할 매도인의 의무는 매수인의 요청에 따라 이루어지는 것이므로 매도인이 매수인의 요청에 따라 보안통관을 위한 서비스나 지원을 제공한 경우 여기에 소요된 비용은 매수인에게 청구할 수 있다.

EXW 조건을 제외한 나머지 규칙에서는 매도인이 자신의 위험과 비용으로

30) Jim Giermanski, The Impact of Incoterms® 2010 on Supply Chain Security Both Global and Domestic, *op. cit.*

수출허가 및 기타 공적인가를 획득하고 수출 및 제3국을 통과하는 인도전의 운송에 필요한 통관절차를 수행하여야 한다. 물품의 통관은 허가(licences), 증명(certificates), 영사송장(consular invoices), 면허(permits), 인가(authorization) 등을 취득하는데 소요되는 비용뿐만 아니라 창고보관료, 세관신고 및 운송주선인의 서비스 비용 혹은 보안관련 정보를 제공하거나 지원하는데 소요되는 비용을 포함한다.[31]

한편, 매도인이 보안통관을 위해 매수인에게 제공하여야 하는 정보는 매도인이 보유하고 있는(in the possession of the seller) 정보에 국한된다. Marcel van Oosterhout[32]은 공급사슬상 정보의 흐름을 내륙운송인, 해상운송인, 화물터미널 등이 포함된 물류계층(logistics layer), 세관 및 검역당국이나 항만당국이 관여하는 정부계층(government layer), 송하인과 수하인을 포함하여 은행, 보험회사, 포워더, 운송대리인 등이 포함된 거래계층(transaction layer)으로 나누어 설명하고 있다. 공급사슬에 참여하는 여러 주체들이 필요로 하는 정보는 다르지만, 공급사슬상 공유되고 관리되는 정보의 원천은 매도인 혹은 송하인으로부터 발생하며, 화물이 매수인 혹은 수하인에게 전달되는 과정에서 공급사슬의 각 단계를 거치면서 부가적인 정보들이 추가되게 된다. 공급사슬의 모든 단계는 상호 연계되어 영향을 주고받기 때문에 각 단계를 서로 구분하기는 어렵지만 송하인 혹은 수출업자는 공급사슬상 다른 어떤 주체보다 수출화물에 대해 더 많은 정보를 가지고 있다. 매도인은 매수인의 주문을 이행하기 위해 계약물품을 준비하고 선적한다. 선적준비가 완료되었을 때 송하인은 거래계층에서 화물 및 관련 당사자들에 관해 이용가능한 모든 정보를 가지게 된다. 이후 단계가 진행됨에 따라 물류계층에서 각 단계별 정보가 부가되는 바, 화물의 이동에 따른 정보의 제공에 각 관련 주체들이 기여를 하게 된다. 따라서 보안통관을 위해 필요하지만, 매도인이 보유하고 있지 않은 정보에 대해서까지 매수인에게 제공할 의무는 없다 할 것이다.

---

31) Jan Ramberg, *ICC Guide to Incoterms® 2010*, ICC, 2011, p. 82.

32) Marcel van Oosterhout, "Organizations and flows in the network", in Peter van Baalen, Rob Zuidwijk and Jo van Nunen, Port inter-organizational information systems: capabilities to service global supply chains, *Foundations and Trends in Technology*, Information and Operations Management, Vol. 2 No. 2-3, 2008, pp. 81-241

2) 매수인의 의무 (B2)

매수인의 의무 B2에서는 DDP 규칙에서조차 보안통관을 위해 요구되는 정보의 제공에 관하여 규정하고 있지 않다. 이는 9/11 테러사건을 계기로 세관의 관리영역이 확장되어 주로 수입국에서 이루어지던 요건확인 및 검사가 수출국가에서 이루어지기 때문인 것으로 볼 수 있다. 과거 수입국 세관은 수입물품에 대한 신고정보를 통해 국경이동 화물에 대한 정보를 관리해왔다. 이러한 관행은 2001년 9.11 테러사태를 계기로 수출입 화물의 제조, 포장 및 선적에 관여한 당사자 및 화물에 관한 확인된 사전정보를 통해 안전 및 보안을 평가하는 형태로 변화되고 있다. 이와 관련하여 송하인은 글로벌 공급사슬상 물류보안요건을 충족하는데 필요한 정보의 주요 원천이 된다.[33] 미국의 24시간 전 적하목록 제출제도나 수입자 보안신고제도, EU의 수입통제시스템(ICS) 등은 주로 수입자 또는 운송인에게 수출국에서 선적이 이루어지기 전 화물보안정보를 제출하도록 의무를 부과하고 있는 바, 신속한 통관 및 효과적인 위험관리가 이루어질 수 있도록 매도인으로 하여금 보안통관에 필요한 정보를 매수인에게 제공하도록 규정한 것이다.

3. 보안관련 정보에 관한 협조 및 비용 상환의무

Incoterms® 2010 규칙 A10과 B10에서는 각각 매도인과 매수인이 상대방의 요청에 따라 상대방의 위험 및 비용부담으로 보안관련 정보를 제공하거나 필요한 지원을 제공할 의무를 규정하고 있다.

1) 매도인의 의무(A10)

EXW 규칙 A10의 경우, 매도인은 매수인의 요청에 따라 매수인의 위험과 비용으로 매수인이 물품의 수출입 및/또는 최종 목적지까지 운송을 위해 필요한 모든 서류와 보안관련 정보를 포함한 모든 정보를 적기에 제공하거나 매수인이 적기에 그러한 서류와 정보를 획득하는데 필요한 지원을 제공하여야 한다고 규정하고 있다.

---

33) David Hesketh, Weakness in the supply chain: who packed the box?, *World Customs Journal,* Vol. 4 No. 2, INCU, Sep. 2010, pp. 3-4.

EXW 규칙상 물품의 수출입, 운송 및 보안통관과 관련하여 필요한 사항은 모두 매수인이 이행하여야 하는 바, 매수인은 이와 관련하여 필요한 서류 혹은 그에 상응하는 전자적 메시지 및 보안관련 정보의 획득을 위해 매도인의 지원을 필요로 한다. 매도인이 매수인에게 보안관련 정보나 지원을 제공하는 것은 매수인의 요청에 따라 이루어지며, 그에 수반하는 위험과 비용은 매수인이 부담하는 것이다.

DDP 규칙 A10의 경우, 매도인은 해당되는 경우 매수인의 요청에 따라 매수인의 위험과 비용으로 지정된 목적지에서 최종목적지까지 물품의 운송에 필요한 모든 서류와 보안관련 정보를 포함한 모든 정보를 적기에 제공하거나 매수인이 적기에 그러한 서류와 정보를 획득하는데 필요한 지원을 제공하여야 한다고 규정하고 있다. 즉, 매도인은 매수인이 지정된 목적지(인도장소)로부터 최종목적지까지 추가운송을 위해 요구되는 필요한 지원을 제공하여야 하며 매수인은 B10의 규정에 따라 매도인이 그러한 지원을 제공하는데 소요되는 비용을 상환하여야 한다.

EXW 규칙과 DDP 규칙을 제외한 나머지 9개 규칙 A10에서는 매도인은 해당되는 경우, 매수인의 요청에 따라 매수인의 위험과 비용으로 매수인이 물품의 수입 및/또는 최종목적지까지의 운송을 위해 필요한 제반 서류와 보안관련 정보를 포함한 모든 정보를 적기에 제공하거나 매수인이 그러한 서류와 정보를 적기에 획득하는데 필요한 지원을 제공하여야 한다고 규정하고 있다.

한편, EXW 규칙을 제외한 나머지 10개의 규칙에서는 매수인이 B10에 규정된 바에 따라 (매도인이 물품의 운송과 수출 및 제3국을 통과하는 운송에 필요로 하는) 서류와 정보를 제공하거나 매도인이 그러한 서류와 정보를 획득하는데 필요한 지원을 제공하는데 수반되는 제반 비용과 부대비용을 매도인이 상환하여야 한다고 규정하고 있다.

EXW 조건상 매도인은 물품의 수출입통관, 운송 및 보안요건의 확인 등과 관련한 직접적인 의무를 부담하지 않으므로, 이러한 의무의 이행을 위해 매수인으로부터 필요한 지원을 제공받을 필요가 없다. 따라서 매수인이 매도인에게 필요한 지원을 제공함에 따른 비용의 상환의무도 없다. 하지만, 매도인은 매수인이 상기와 같은 의무를 이행하도록 필요한 한 지원을 제공해줄 의무가 있으며, 그에 따른 비용은 매수인이 매도인에게 상환하여야 한다.

하지만, EXW 규칙을 제외하고 매도인은 개별 규칙에 따라 물품의 수출허

가, 운송 및 제3국을 통과하는 운송의무를 이행하여야 하는 바, 매도인이 그러한 의무를 이행할 수 있도록 매수인이 B10의 규정에 따라 필요한 지원을 제공하는 경우, 매도인은 매수인이 그러한 지원을 제공함에 따라 수반된 비용을 매수인에게 상환하여야 한다.

DDP 규칙의 경우 매도인으로 하여금 수입통관을 하도록 요구하고 있다. 하지만, 매도인의 요청이 있는 경우, 매수인은 매도인이 수입통관을 위해 필요한 모든 서류 혹은 보안관련 정보를 포함한 모든 정보를 획득하는데 필요한 지원을 제공하여야 한다. 이 경우 매도인은 매도인의 요청에 따라 매수인이 필요한 지원을 제공하는데 소요된 모든 비용을 상환하여야 한다.

2) 매수인의 의무(B10)

Incoterms® 2010의 11개 규칙 모두 B10에서 매수인은 매도인이 A10의 규정에 따른 의무를 준수할 수 있도록 모든 보안정보요건들을 적기에 매도인에게 통지하여야 하며, 매도인이 A10에 규정된 바대로 [매수인이 필요로 하는] 서류와 정보를 제공하거나 그러한 서류와 정보의 획득에 필요한 지원을 제공하는데 수반되는 모든 비용과 부대비용을 매도인에게 상환하여야 한다고 규정하고 있다.

A10의 규정에 따라 매도인은 매수인이 물품의 운송, 수입 및 보안통관을 위해 필요한 서류나 그에 상응하는 전자적 메시지 및 정보를 획득하는데 필요한 지원을 제공하여야 할 의무가 있다. 하지만, 이러한 지원은 어디까지나 매수인의 위험과 비용부담으로 이루어지는 것인 바, B10에서는 매도인이 그러한 지원을 제공하는데 수반되는 제반 비용과 부대비용을 매수인이 지급하여야 함을 규정하고 있으며, 매도인이 그러한 비용을 지급하였다면 당해 비용을 매수인이 매도인에게 상환하여야 한다. 또한, 매수인은 매도인이 [세관 및 기타 관계 당국에서 요구하는 보안절차를 이행하는데] 필요한 지원을 [적기에] 제공할 수 있도록 보안요건의 확인에 필요한 모든 정보를 매도인에게 통지해 주어야 한다.

EXW 규칙을 제외한 나머지 10개의 규칙에서는 상기 규정에 추가하여 매수인은 해당되는 경우, 매도인의 요청에 따라 매도인의 위험과 비용부담으로 매도인이 물품의 운송과 수출 및 제3국을 통과하는 운송에 필요한 제반 서류와 보안관련 정보를 포함한 정보를 적기에 제공하거나 그러한 서류와 정보를 획

득하는데 필요한 지원을 제공하여야 함을 규정하고 있다.

EXW 규칙의 경우 매수인이 물품의 수출입 및 운송의무를 부담하므로, 매수인이 매도인에게 필요한 제반 서류나 정보를 제공하거나 매도인이 그러한 서류나 정보를 획득하는데 필요한 지원을 제공할 필요가 없다. 반대로, 그러한 제반 서류나 정보의 제공 및 지원은 매수인의 요청에 따라 매수인의 위험과 비용으로 매도인이 제공해야할 것이며, 매수인은 그에 수반되는 비용을 매도인에게 상환하여야 할 것이다.

4. 보안통관 관련 위험 및 비용의 분담

1) 보안통관절차의 이행에 따른 위험의 분담

경우에 따라서는 매도인이 자신의 인도의무를 이행하기 전에 매도인으로부터 매수인에게로 위험이 이전할 수 있다. 매도인이 매수인에게 물품을 인도하기 위해서 매수인에게 요구되는 조치들을 취하지 않거나 매수인이 물품의 인도수령을 거부하는 경우 등이 이러한 경우에 해당한다.

따라서 매수인은 매도인이 물품의 인도를 준비하는데 필요한 사항들을 통지해주거나 계약에서 약정한 대로 운송인으로부터 물품의 인도를 수령하여야 한다. 또한 매수인이 물품의 수입통관의무를 부담하는 경우 매도인이 예정된 목적지까지 후속운송을 진행할 수 있도록 합의된 기간 내에 이러한 의무를 수행하여야 한다. 그렇지 않은 경우 매수인은 그로 인해 발생하는 물품의 멸실 또는 손상의 모든 추가적인 위험을 부담하여야 한다.

매수인이 보안통관에 필요한 요건을 충족하지 못하였거나, 매도인이 수입국에서 요구하는 보안통관에 필요한 정보 및 지원을 매수인이 적시에 제공하지 않아 선적이 보류되거나 통관이 지연되어 인도가 늦어지는 경우, 인도전이라도 위험이 매수인에게 이전할 수 있다.

또한 보안통관은 매도인과 매수인 상호 간의 협력이 필요한 부분으로 매수인이 B10의 규정에 따라 보안통관에 필요한 사항들을 매도인에게 적기에 통지할 의무는 매도인이 A10의 규정에 따라 매수인에게 보안통관을 위한 정보를 제공하거나 필요한 지원을 제공할 수 있도록 하기 위한 전제조건이 된다. 따라서 매도인이 매수인의 요청에 따라 매수인이 요구하는 물품의 보안통관에 필요한 정보를 적기에 제공하였음에도 불구하고 세관이나 관계당국의 보안요

건을 충족하지 못함으로 인해 발생하는 과징금의 부과나 선적보류 및 통관지연 등의 위험은 매수인이 부담하여야 한다. 다만, 매수인이 요구한 보안관련 정보가 누락되거나 그러한 정보가 적기에 제공되지 못함으로 인하여, 예컨대 선적 24시간 전 등, 발생하는 위험 및 비용은 매도인이 부담하여야 할 것이다. 미국의 매수인(수입자)이 10+2 Rules에 따라 선적 전 자동적하목록시스템을 통해 보안정보를 제출하였음에도 중대한 위반사항이 발견되어 운송인에게 적재불가(Do Not Message)가 전송되는 경우 FOB나 CIF 규칙상 매도인은 화물을 본선에 적재할 수 없게 된다. 만일 매도인이 매수인이 요청한 정보를 누락하거나 제공한 정보 상에 오류가 있는 경우, 또는 정보제공 시기를 지키지 못한 것이 적재불가의 원인이 된 경우 매도인은 인도지연에 따른 위험 및 책임을 부담하여야 할 것이다. 반면, 적재불가의 원인이 매수인이 보안통관에 필요한 사항들을 적기에 통지하지 않은데 있는 경우 선적 전이라도 물품에 대한 멸실 또는 손상의 위험은 매수인에게 이전하게 된다.

2) 보안통관절차의 이행에 따른 비용의 분담

대부분의 경우, 별도의 약정이 없는 한 일방 당사자가 계약상 담당하게 되는 의무로 인해 발생되는 비용은 당해 의무를 이행하는 당사자가 부담한다. 하지만, Incoterms® 2010 규칙상 매매당사자의 보안관련 의무는 상대방의 요청에 따라 부담하게 되는 의무이다. 따라서 매도인과 매수인은 각각 상대방의 요청에 따라 보안통관에 필요한 서류와 정보를 제공하거나 그에 필요한 지원을 제공할 의무를 부담하되, 당해 의무의 이행과정에서 발생하는 비용은 상대방으로부터 보상받을 수 있다.

일부 국가에서는 수입허가를 위해 관계당국에서 선적 전 검사를 요구할 수 있다. 이러한 검사는 통상적으로 관계당국이 지정한 검수회사에 의해 이루어지며, 검사비용은 해당 기관에서 지급한다. 하지만, 매매 당사자 간에 별도의 약정이 없는 한, 해당 기관이 지급한 검사비용은 매수인이 상환하여야 한다. 미국은 컨테이너보안협정(CSI) 및 항만보안법(SAFE Port Act)에 따라 외국 항만에서 선적 24시간 전에 미국 세관원이 현지국 세관원과 공동으로 미국행 컨테이너 화물의 사전검색을 실시하고 있다. 이러한 검사에 소요되는 비용은 미국의 국내법에 따라 수입허가를 위해 필요한 검사이므로 매수인이 부담하여야 할 것이다. 또한 물류보안 강화에 따른 선사나 항만당국의 보안설비 투자가

불가피해짐에 따라 보안할증료[34]를 징수하는 경우, 이러한 비용의 부담주체에 대해서 매매당사자 간 합의가 도출되어야 할 것이다.

통관절차의 지연 등 예견할 수 없었던 사건으로 인해 추가적인 비용이 초래되는 경우 비용의 분담과 관련하여 어려움이 발생한다.[35] 수입국 세관에서 요구하는 보안관련 정보를 정해진 시간 내에 제출하지 못하거나 허위정보를 제출한 때에는 관계 법령에 따라 벌금이 부과되거나 선적이나 양륙허가가 보류될 수 도 있고, 현물검사과정에서 추가적인 비용이나 지연이 발생할 수도 있다.[36] 공항이나 항만으로부터 내륙으로의 연계운송이 원활히 작동하지 않는 경우 기업의 생산계획이나 배송계획에 차질이 발생하게 되고, 이는 결국 재고수준 및 처리비용의 증가로 이어져 기업의 운전자금 및 현금흐름에도 영향을 미치게 된다.[37] 뿐만 아니라 검사과정에서 컨테이너 화물의 손상이 발생하는 경우 그 비용은 고스란히 운송인과 수입자가 떠안게 된다. 보안통관 과정에서 직접 혹은 간접적으로 추가적인 비용이 발생하게 되는 경우 당해 비용을 누가 부담할 것인지는 귀책사유가 누구에게 있는지를 따져서 결정해야 할 문제이다. 한편, 매도인과 매수인 간에 Incoterms 2010 규칙에 따라 매매계약을 체결한 경우 당사자 일방이 통관과정상의 혜택을 누리기 위해 물류보안인증 요구할 경우 AEO 인증절차에 소요되는 비용의 분담 등도 매매 당사자 간에 합의가 필요한 부분이다.[38]

---

34) EU의 주요 항만들은 컨테이너 당 8-10 Euro의 보안할증료를 부과하고 있고, 캐나다의 경우 TEU당 2달러, FEU당 4달러의 보안할증료를 부과하고 있다.

35) Jan Ramberg, *op. cit.*, p. 80.

36) 미국의 사전 적하목록 제출규정에 따르면 최초 위반 시 미화 5천 달러의 벌금이 부과되며, 그 이후에 계속 위반 시에는 1만 달러의 벌금과 선박의 억류나 몰수조치가 취해질 수 있다. 또한 사전 적하목록 제출규정 위반으로 도착지에서 미국 세관이 관리대상화물로 지정하여 직접 검사를 하는 경우 TEU당 300 ~ 500달러의 비용이 발생하게 된다. 또한 화물을 반송하게 될 경우 TEU당 3천달러의 추가비용이 발생한다고 한다(허은숙, "미국 물류보안 규범이 우리나라의 공급망 참여자에게 미치는 영향과 대응방안", 통상정보연구 제10권 제1호, 2008. 3., p. 230.).

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

38) AEO 시범사업에 참여 할 경우, 보안시설 4천만 원의 투자비용뿐만 아니라 인적자원과 준비기간이 소요된다. 또한 미국의 사전적하목록 제출제도에 따른 AMS charge는 B/L 건당 미화 25-50달러가 소요된다(이주원 · 최혁준 · 최문성, 한국수출업체의 물류보안 인식 및 리스크 관리방안, 정석물류통상연구원 연구총서, 10-03, 2010p. 90.).

Ⅳ. 시사점 및 결론

글로벌 공급사슬보안요건이 강화됨에 따라 세관당국의 역할은 관세의 징수에서 공급사슬 보안 및 수출입 세관당국 간의 협력으로 변화하고 있다. 미국의 C-TPAT를 비롯하여 EU의 AEO제도, 캐나다의 PIP, 싱가포르의 STP 등 세계 각국의 물류보안프로그램들에 의해 이러한 변화가 입증되고 있다. 이러한 세관당국의 역할 변화가 Incoterms 규칙에 미치는 영향은 자명하다. 매도인과 매수인은 수출입 물품의 통관의무를 분담하되, 사전 적하목록 제출이나 수입자 보안신고와 같이 사전에 요구되는 정보를 제공하기 위한 지원이 필수적인 요건이 되었으며, 경우에 따라서는 화물의 보안위험 탐지를 위한 검사(inspection)를 받아야 한다. 이러한 지원은 물품의 통관의무를 부담하는 당사자의 위험과 비용 하에 이루어지기 때문에 WCO SAFE Framework에 규정된 혜택을 누리기 위한 파트너의 선정 및 관련 세관당국에서 시행하는 보안프로그램의 준수가 지상과제가 되었다.[39] 따라서 매매당사자들은 Incoterms® 2010상 보안관련 의무의 이행을 위해 다음과 같은 사항에 유의해야 한다.

첫째, Incoterms® 2010이 시행되기 전 매도인과 매수인은 수출입 통관상의 혜택을 누리기 위해 혹은 장기적으로 지속적인 거래관계의 유지를 위해 보안관련 정보 및 보안에 필요한 조치들을 제공하였으나, Incoterms® 2010의 시행으로 이는 매도인과 매수인이 상호 간에 부담하여야 할 필수적인 의무가 되었다. 따라서 매매당사자가 Incoterms® 2010 규칙상 보안관련 의무를 제대로 이행하지 못한 경우 그로 인해 발생하는 손해에 대한 배상책임을 부담해야만 한다. 수출입 통관과정에서 요구되는 보안요건을 충족하지 못함으로 인해 초래되는 손해는 선적보류, 통관지연, 검사 과정에서 화물의 손상, 과징금의 부과, 생산 및 배송차질 등 다양하다. 이러한 손해는 그 액수를 명확히 산정하기 어려운 경우가 많다. 따라서 보안관련 의무의 위반으로 인한 손해에 대해서는 손해배상액 예정조항(liquidated damage clause)을 통해 배상액을 미리 합의해 둘 필요가 있다.

둘째, 물류보안 인증에 따른 다양한 혜택을 누리기 위해 C-TPAT에 가입한

---

39) Incoterms® 2010, International Chamber of Commerce, 2010, p. 68

미국의 수입자들은 한국의 수출자 등에게 C-TPAT 인증을 취득하도록 요구하거나 C-TPAT의 안전기준을 준수하도록 요구하는 사례가 많이 발생하고 있다.[40] 수입자의 요청에 따라 수출자가 물류보안인증을 취득하는 경우 그에 따른 편익은 주로 수입자에게 제공된다고 볼 수 있다. 하지만 물류보안인증은 수입자와 좋은 거래 관계를 지속하고 장기적으로 수출자의 경쟁력을 높일 수 있는 방편이 되기도 한다. 따라서 수출기업들은 물류보안인증을 취득하기 위해 적극적으로 노력해야 할 것이다.

셋째, 사전 전자정보 제출규정과 관련하여 매도인은 수입국에서 요구하는 보안신고 사항을 적시에 수입자 또는 운송인에게 제공할 수 있도록 관련 자료를 미리 확보함으로써 선적에 차질이 발생하지 않도록 하여야 할 것이다. 구체적으로 선사에서 선적 24시간 전 적하목록을 신고하기 위해 송하인은 선적 72시간 전 적하목록에 관한 정보를 선사에 제공하여야 하고, 화물마감시간이 단축됨에 따라 수출물품의 조달계획이나 화물반입시간을 철저히 관리해야 한다. DDP 조건의 경우 매도인이 직접 관련 내용을 확보하여 수입통관 등의 공적절차를 수행하여야 하는 바, EU의 경우 보안관련 정보를 운송인이 제출하게 되므로 매도인이 운송인에게 관련정보를 제공해 주어야 하며, 미국의 ISF의 경우 수입업자가 ISF를 전송해야 하므로 미국내 ISF 전송 대리인을 미리 확보해 두어야 한다.[41]

넷째, 미국의 사전 적하목록 신고제도의 경우 어떠한 경우든 화물명세가 공란으로 남겨지거나 'Freight All Kinds (FAK)', 'Said To Contain (STC)', 'General Merchandise', 'Consolidated Cargo' 등 상품명이 분명하지 않거나 일반적이고 애매한 표현은 허용되지 않는다. 따라서 보안신고 과정에서 오류가 발생하기 않도록 화물의 명세를 구체적이고 명확하게 기술하여야 한다.

마지막으로, 매매당사자의 보안관련 의무는 Incoterms® 2010의 개별 규칙에 따라 결정된다. 하지만, 보안관련 의무의 이행에 따른 책임관계를 명확히 하기 위해서는 수출입 당사자가 제공해야 할 정보 및 서류목록, 그리고 물품

---

40) 송선욱, "무역원활화와 국경안전 강화를 위한 세관과 업계의 협력 사례분석과 그 시사점", 무역학회지 제31권 제5호, 2006. 11., p. 255

41) 송선욱, "세관 사전전자정보 제출과 Incoterms 2010 보안관련 정보제공의무 규정과의 관계", 관세학회지 제12권 제1호, 2011. 2., p. 63

의 제조, 포장, 선적, 운송 및 인도 과정에서 당사자 상호 간에 부담해야 할 구체적 내용에 대해 합의할 필요가 있다. 가령, 운송계약을 매도인이 체결하는 C 규칙이나 D 규칙의 경우 선적항이나 운송인의 선정이 수입국에서 요구하는 보안기준의 충족에 영향을 미칠 수 있는 바, 매도인이 ISPS Code나 항만보안법 등에서 규정하고 있는 보안시스템이나 설비를 갖춘 항만이나 선사를 이용하도록 계약상 약정할 필요가 있다.

참 고 문 헌

고현정, "국제물류보안인증제도 동향 및 시사점에 관한 연구", 한국항만경제학회지 제27집 제2호, 2011, pp. 333-54.

김창봉 · 천홍욱, "AEO제도 구축과 물류공급체인망 성과에 관한 연구", 유통경영학회지, 제13권 제1호, 2010, pp. 107-131.

박찬석, "국제 물류보안 동향과 시사점", 우정정보 82, 2010 가을, pp. 29-64.

송선욱, “무역원활화와 국경안전 강화를 위한 세관과 업계의 협력 사례분석과 그 시사점”, 무역학회지 제31권 제5호, 2006. 11., pp. 239-259

_____, “세관 사전전자정보 제출과 Incoterms 2010 보안관련 정보제공의무 규정과의 관계”, 관세학회지 제12권 제1호, 2011. 2., pp. 45-65.

이주원 · 최혁준 · 최문성, 한국수출업체의 물류보안 인식 및 리스크 관리방안, 정석물류통상연구원 연구총서 10-03, 2010.

최재선, 컨테이너화물 100% 사전검색 의무화와 정책시사점, KMI 해양수산 현안분석, 2007-14.

한상현 · 최준호, WCO 표준(Standards)에 대응하기 위한 각국의 보안조치 강화 방안, 관세학회지 제8권 제4호, 2007, pp. 75-93

허은숙, “미국 물류보안규범이 우리나라의 공급망 참여자에게 미치는 영향과 대응방안”, 통상정보연구 제10권 제1호, 2008. 3., pp. 217-236.

관세청, AEO 가이드북, 2009, p. 10

KEIT, 화물컨테이너용 보안장치 기술동향 및 국제 표준화 이슈, KEIT PD Issue Vol. 10-2, p. 21

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

Gardner Dan, A New Chapter in Incoterms, The Journal of Commerce, Sep. 15, 2008, p. 60.

Giermanski Jim, The Development and Globalization of Container Security, Defence Transportation Journal, September 2008, pp. 16-22

_____, The Impact of Incoterms® 2010 on Supply Chain Security Both Global and Domestic, The Maritime Executive,

May 11, 2011 (http://www.maritime-executive.com)

_____, Tracking and Chain of Custody: The Difference, The Maritime Executive, November 17, 2011 (http://www.maritime-executive.com)

Ireland Robert, The Customs Supply Chain Security Paradigm and 9/11: Ten Years On and Beyond, WCO Research Paper No. 18, Sep. 2011

Lowe David, Incoterms 2010: Making trading easier, Practical Law for Companies, Vol. 21. Part 9, 2010, pp. 11-13

Merritt David, The EU's new import control system - creating supply chain chaos, Trade & Forfaiting Review, Vol. 13 Issue 7 (www.tfreview.com)

Oosterhout Marcel van, "Organizations and flows in the network", in Peter van Baalen, Rob Zuidwijk and Jo van Nunen, Port inter-organizational information systems: capabilities to service global supply chains, Foundations and Trends in Technology, Information and Operations Management, Vol. 2 No. 2-3, 2008, pp. 81-241

Ramberg Jan, ICC Guide to Incoterms® 2010, ICC, 2011

Richer Suzanne, Balancing Global Priorities, Logistics Management, January 2011, p. 43

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

Incoterms® 2010, International Chamber of Commerce, 2010, p. 9

WCO, WCO SAFE Framework of standards, June, 2011, p. 21

ABSTRACT

A Study on the Security related Obligations of Contracting Party under the Incoterms® 2010 Rules

Yang, Jung-Ho

Since the 9.11 terror attack, the event which caused supply chain disruption, supply chain security has become more important than ever before. With this as a momentum, a customs supply chain security paradigm emerged intended to guarantee secure flow of cargo across boarder. Under this circumstances Incoterms® 2010 rules have allocated obligations between the buyer and seller to obtain or to render assistances in obtaining security clearances. Thus, security related obligations such as providing advance manifest information is the mandatory requirements for any export and import.

The impact on the seller and buyer of security related obligations under the Incoterms® 2010 rules environment is obvious. Assistance to provide the security information in advance has become indispensable obligations to the seller and buyer. As such assistances is at the cost and risk of the party responsible for the clearances of the goods, the choice of recognised partner and compliance with the relevant security program, in order to enjoy the relevant benefits, becomes paramount.

Key Words : Incoterms® 2010, Security related Obligations, Security Clearance, Supply Chain Security, Logistics Security, AEO, C-TPAT