



### 기술표준동향

# 글로벌 물류보안 환경 변화 및 물류보안표준

## I. 글로벌 물류보안 환경의 변화

국제 테러 위협의 증가로 항공기, 선박 등에 대한 보안검색이 강화되면서, 미국, 유럽 및 국제기구에서는 물류보안 강화에 따른 다양한 제도를 추진하고 있다. 미국의 Safe Port Act에 의한 컨테이너 안전협정(Container Security Initiative), 세계관세기구(WCO)의 무역 안전 및 원활화에 관한 표준틀(Framework of Standards to Secure and Facilitate Global Trade) 및 국제해사기구(IMO)의 선박 및 항만시설 보안에 관한 규칙(International Ship and Port Facility Security)이 대표적인 예이다.

또한 이러한 글로벌 물류보안 환경 변화 속에서 새로운 무역 장애요인 해소를 위한 국내 물류업계의 노력도 다각적으로 이루어지고 있다. 원활한 대미 수출을 위하여 부산항도 CSI에 합의하고, 미국행 선박에 대해 미국 세관 직원과 우리나라 세관 직원이 공동 검색을 실시하고 있으며, 국제선박보안인증서 소지 의무화에 따른 ISPS 인증도 국토해양부에서 실시하고 있다. 또한 관세청에서는 한국, 벨기에 간 보안장치(CSD)의 통관정보 교환 시범사업을 추진하여, 수출품의 통관 지연 또는 선적금지, 추가 검사비용 부담 등 피해를 최소화 할 수 있는 글로벌 물류보안 인증체제를 구축하고자 노력해 왔다.

그러나 물류보안 제  
제구축은 물류보안  
의 적용범위나 내용  
선략 측면에서 본 때  
특정 정부기관에서  
의 역할로 국한하여  
집단하기에는 이제  
지원이 다른 분계이  
나, 한 국가 안에서도  
물류보안은 해상 운  
송, 항만하역, 통관  
뿐만 아니라 제조업,



**윤종구**  
여니시물류표준과 과장  
02-609-7270  
kyoon@nke.go.kr

운송업 등 물류전반에 걸친 물류공급사슬(Supply Chain)에서 연계된 통합적인 보안은 요구하고 있다. 화물의 부결합, 보안장비 및 시설의 원비, 경영자의 물류보안 의식 고취, 관계자의 물류보안 교육훈련, 물류보안 경영시스템의 구축 등 장비, 시스템, 교육, 훈련 및 경영에 이르기까지 통합적인 물류보안을 요구하는 단계에 이르고 있다.

이러한 물류보안 환경의 특징을 고려하면 산업계에서도 글로벌 물류보안 환경 변화에 대한 정확한 이해가 전제되어야만, 이에 대한 적절한 대응 방안을 수립할 수 있다. 이하에서는 물류보안정책에 대하여 살펴봄으로 글로벌 물류보안 환경변화에 대한 이해도를 높이고자 한다.

## 1. 미국의 물류보안정책

9.11 테러 이후의 글로벌 물류보안 강화 움직임의 주역인 미국은 신속한 자국내 제도를 도입하고, 민간단체, 교역 국가 및 국제기구와의 적극적인 협력을 통해 글로벌 물류보안체제 강화를 주도하고 있다. 특히, 2003년 해운보안법, 2006년 항만보안법을 제정한 후 2007년 9.11 테러대책 이행법률을 제정하면서 자국으로 수출되는 모든 컨테이너 화물을 100% 검색하는 제도를 도입하는 등 물류보안정책에 대한 다각적인 접근을 이행하고 있다.

미국 내 항만 및 운하의 테러 공격을 방지하기 위해 만들어진 해운보안법(MTSA; Maritime Transportation Security Act, 2002)은 항만 및 선박의 위협에 대한 보안 평가와 외국항만에서의 보안평가를 두루 포함하는 법으로, 2003년 7월부터 해운보안위원회(maritime security committee) 설치와 항만시설 및 선박에 대한 보안계획(security plan)을 요구하고 있다. 이 보안계획서에는 치명적인 인명의 손실, 환경훼손, 운송시스템의 중단, 특정지역에 대한 경제혼란을 야기하는 운송보안사고(transportation security incident)에 대한 보안계획을 수립하도록 규정하고 있다. 또한 승객, 선박 및 화물에 대한 검색 절차, 보안 순찰, 제한구역 설정, 개인 확인 절차, 통제법 평가, 귀시 장비 설치 등도 포함하고 있다. 해운보안법은 형식적으로는 국제해사기구의 "국제선박 및 항만시설 보안 규정(ISPS)"과 그 내용을 같이 하고 있지만, 실질적인 측면에서는 미국으로 출항하는 2500여개 외국 항만에 대한 보안조치의 시행 여부를 관리할 수 있는 법적 기반을 마련하였다.

또한 인증제도로는 반테러 민관협력제도(C-TPAT; Customs-Trade Partnership Against Terrorism, 2002)를 운영하고 있다. 이 제도에서는 물류공급사슬에 가장 핵심적인 관계자인 수입

업자, 선사, 통관승개업자, 창고업자, 제조업자 등 개인 사업자와의 협력을 핵심으로 개인 사업자가 보안개선 프로그램을 개발하여 미국 세관에 승인을 받으면, 신속통관, 낮은 검색율, 관세 지불의 전자질차 등의 혜택을 부여하는 자발적인 물류보안인증제도의 성격을 가지고 있다.

화물 컨테이너에 대한 보안조치는 컨테이너 보안대책3(CSI; Container Security Initiative, 2002), 24시간 규칙(24 Hour Advance Cargo Manifest Declaration Rule, 2003) 및 주요항만관리협정(The Megaports Initiative)에 의해 핵무기, 탄저균과 같은 대량사상무기 등이 선박 컨테이너를 통해 미국 내에 반입되는 것을 방지하기 위한 조치로부터 시작되었다. 세관국경보호국(CBP; Customs and Border Protection)에서 추진하고 있는 컨테이너 보안대책(CSI)에서는 미국 세관원이 외국 항만의 세관원과 협력하여 화물을 선적하기 24시간 전에 검색할 수 있도록 하고 있으며, 위험 화물로 간주되어진 경우 화물을 열고, X-선 검색을 하며, 위험성이 낮은 컨테이너의 경우 통관을 효율적으로 진행하는 화물의 위험성에 따른 선별적인 검색을 추진하고 있다. 24시간 규칙에서는 미국행 화물에 대하여 선적 24시간 전에 적하 목록 또는 화물리스트를 제출하도록 하고 있다. 이 규칙의 시행 초기에는 선박에 대해서만 적용되었으나, 철도는 도착 2시간 전, 항공은 1시간 전, 트럭과 같은 자동차는 30분에서 1시간 전에 제출하는 것으로 확대 운용되고 있다. 또한 주요항만관리협정에서는 각국 주요항구에 핵물질 탐지 장비를 설치, 출입하는 모든 컨테이너를 감시하도록 규정하였다.

미국의 화물에 대한 보안검색제도는 2006년 제정한 항만보안법(SAFE Port Act; Security and Accountability For Every Port Act)과 이에 대한 세부조치인 10+2 조치(Ten plus Two data elements required by the U.S. Customs and

Border Protection) 및 화물운송 안전조치 (Seure Freight Initiative, 2006)로 더욱 강화되고 있다. 항만보안법에서는 2007년 말까지 미국의 22개 주요 항만에서 모든 수입 컨테이너 화물에 대한 핵물질 검색이 이루어진 것이며, 외국의 3개 시범항만에서 통합 검색 시스템에 대한 시범사업을 규정하고 있다. 이법의 세부조치로 이루어진 화물운송 안전조치(SFI)에서는 파키스탄의 카श्, 영국 사우스햄튼, 온두라스의 푸에르토코르테스 항만에서는 100% 화물 검색을, 한국 부산 감만터미널, 싱가포르, 오만의 살라라 항만, 홍콩 모던터미널에서는 부분 검색을 실시하여 컨테이너 내부 데이터와 이미지를 미국 세관국경보호국의 타게팅센터(National Targeting Center of the U.S Customs and Border Protection)로 송부하도록 하고 있으며, 화물의 안전이 확인되기 전에는 어떠한 화물도 선박에 선적될 수 없도록 하고 있다. 또한 10+2 조치에서는 24시간 규칙의 보안 조치 성격으로 제조업자의 이름 및 주소, 바이너의 이름 및 주소 등 화주에 관한 10개 데이터와 선박 직재 계획 및 컨테이너 상태 등 해양 운송 데이터 등을 24시간 전에 제출하도록 하고 있다.

미국의 CBP를 중심으로 추진하고 있던 컨테이너 화물 검색제도와는 별개로 미국 의회에서는 컨테이너 100% 사전검색제도에 대한 9.11 테러 대책 권고 이행법(Implementation Recommendations of the 9.11 Commission Act, 2007)을 2007년 8월 입법화 하였다. 이 법에서는 모든 미국행 항공 화물은 2009년말 까지, 컨테이너 적재 선박에 대해서 2012년 2월까지 컨테이너가 적재되는 외국 항만에서 X선에 의한 컨테이너 내부 이미지 검색 및 방사선 검색을 의무화하고, 이를 이행하지 않을 경우 미국 입항을 금지하도록 규정하고 있다.

## 2. 국제해사기구의 선박·항만 보안제도

가장 대표적인 선박 및 항만 보안제도인 "국제선박 및 항만시설 보안에 관한 규칙(ISPS; International Ship and Port Facility Security Code)"은 국제해사기구(IMO; International Maritime Organization)에서 2001년 7월부터 시행한 국제규범으로 선사 및 항만 당국, 계약국 정부에서 선박 및 항만의 보안을 확보하기 위해 국제 항해에 종사하는 모든 선박은 제약국의 관청에서 승인한 선박보안계획을 비치하도록 하고 있다. 이 코드의 접근 방법은 리스크 관리 방법의 확보, 적절한 보안조치 확보 및 개별적인 상황에 대한 리스크 평가를 포함하고 있다. 따라서 항만시설 및 선사도 보안계획을 수립하여야 하며, 선사는 선박마다 선박보안담당관 및 회사보안 담당관을 지정하여야 한다. 또한 국제해사기구에서는 2008년부터 500톤 이하 선박에도 적용하는 방안과 장거리 선박 위치추적 시스템 설치를 의무화하는 방안을 검토하여 ISPS code의 실효성을 높이고자 노력하고 있다.

## 3. 세계관세기구의 물류보안정책

세계관세기구(WCO; World Customs Organization)는 회원국의 98%가 근로별 무역을 행하고 있기에 국제 세관규격의 개발, 세관절차의 간소화 및 조화, 물류사슬 내에서의 보안, 글로벌 교역 촉진 등을 위하여 다양한 글로벌 교역 활성화 방안을 장구하고 있다.

2002년 미국의 CSI를 실시하고, 같은 해 6월 「교통보안에 관한 GS 협조행동」의 합의 등이 배경이 되어, 2004년 6월의 WCO총회에서도 「국제무역 Supply Chain의 안전 확보 및 원활화에 관한 WCO결의」가 채택되었다. 이에 대한 실행지침으로 세계관세기구는 각국의 세관당국과 민간업체가 근로별교역의 안전 및 원활화에 관한 각종 표준을 좀 더 쉽게 이해할 수 있도록

록 하기 위해 2006년 "무역 안전 및 원활화에 관한 표준틀(SAFE Framework: Framework of Standards to Secure and Facilitate Global Trade)"<sup>6</sup>을 제정했다. SAFE Framework의 근간이 되고 있는 개념은 미국의 CSI, 24시간 규칙, C-TPAT과 EU의 화물정보 사전제출, AEO, 세관 간에 Risk 정보 공유, 그리고 WCO의 ISCM 가이드라인이 그 중요한 부분을 차지하고 있다. 따라서 SAFE Framework의 목적은 국제적으로 표준화된 기준을 제시하고 이를 실시함으로써 국제무역에서의 확실성과 예견가능성을 촉진하게 하며, 모든 수출수단에 대하여 통합된 공급사슬 관리를 가능토록 하여 세관의 역할, 기능 및 능력을 향상시키는 것이다. 이에 대하여 세관상호의 협력(Customs to Customs)에서는 세관당국의 통합 공급사슬 관리를 위한 세관관리 절차의 실시, 화물검사 권한 부여, X선 검색기 설치, 리스크 관리시스템 확립, 높은 리스크 화물 분리, 사전 전자정보 제공, 표준화된 정보 정보교환 방법 사용, 탈성도 조사, 안전평가, 직원 훈련 교육 및 수출안전점사의 11항목을 세관과 민간과의 파트너십(Customs to Business)의 측면에서는 파트너십, 안전확보, 인정, 기술적용, 커뮤니케이션 및 무역원활화의 6항목 표준을 규정하고 있다.

#### 4. ISO, EU, 관세청, Singapore 등의 물류보안인증제도

물류보안 인증제도의 기본은 물류보안 수준을 향상시킨 무역업자에게 통관 등에 필요한 절차 등을 간소화하는 방향으로 무역 촉진을 도모하고자 하는 제도로서 2002년 미국의 반테러 민관협력제도(C-TPAT)에서 시작되어, 2005년 글로벌 표준화기구(ISO)의 물류공급사슬보안경영인증제도(ISO/PAS 28000), 2006년 세계관세기구(WCO)의 글로벌 교역의 안전과 간소화를 위한 기준(SAFE Framework), 2007년 싱가포르의 안전교역협력프로그램(STP), 2008년 유럽연합

(EU)의 공인경제운영자(AEO) 등 민간기관의 물류보안체제 구축의 참여를 유도하는 다양한 인증제도가 세계기구나 각 국에서 추진되고 있다.

이들 다양한 물류보안인증제도는 제도마다 상이한 부분을 가지고 있기는 하지만 전체 물류공급사슬 내에서 보안 및 교역 원활화를 동시에 추구하겠다는 기본 이념 하에 검색설비 구축, 정보제공, 리스크 평가, 관련자의 교육훈련 등을 통한 안전한 보안체제를 구축할 수 있는 표준을 제공하고, 이를 준수한 신뢰할 만한 무역업자(AEO)에게 혜택을 부여하겠다는 것이 핵심이다. 여기서는 가장 대표적인 인증제도인 유럽연합의 AEO 제도에 대해 상술하기로 한다.

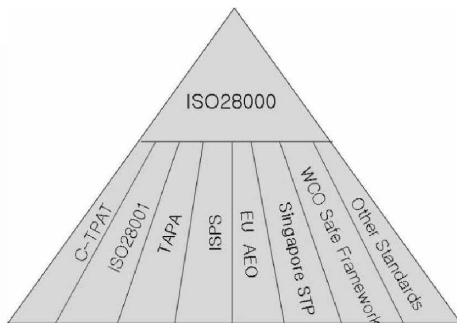
공인경제운영자(AEO) 제도는 유럽공동체 국경을 넘나드는 화물에 숨겨진 나쁜 위험 분석을 위한 기준을 제공하여, 2008년 1월 부터 보안 관련 규정을 철저히 준수해 온 신뢰할 만한 무역업자(AEO)에게 혜택을 부여하게 된다. 주어지는 두 가지 혜택으로는 집중화된 통관절차 또는 면제 등 세관 규정에 의해 주어지는 절차 간소화와 보안 관련 원활화의 혜택으로 구분되므로, AEO 자격 역시 두 가지로 구분된다. 세관간소화의 절차만을 위한 경우 AEO는 재정 건정성, 세관 요구조건 이행의 적절한 기록, 적절한 세관의 통제를 가능하게 하는 상업거래 및 운송 기록 관리 시스템 등에 관한 요구 조건을 준수하면 이에 해당하는 AEO 자격을 부여하며, 보안 간편화 혜택을 원하는 AEO는 사업장이나 출하장소에 대한 보안조치에 관한 요구조건만을 충족시키면 된다. 또한 EU 이외의 국제 무역을 주로 하는 무역업자는 간소화 및 원활화를 둘 다 요구할 수 있으므로 두 가지 요건을 충족한 AEO 지위를 획득할 수 있다. AEO 제도는 글로벌 수준의 상호 인정의 기본 틀을 마련하여, 리스크가 높은 사업자를 집중적으로 관리함으로써 국제 물류공급사슬의 안전 및 보안을 확보하고, 기준을 잘 준수하는 우수 사업자에게 거래

의 편의를 제공함으로써 무역 활성화를 구현하겠다는 세관 통제 정책을 실현 한 대표적인 예로 평가 받고 있다.

## II. 국제표준화기구의 물류보안표준 동향

### 1. ISO 28000 물류보안 인증제도

미국의 C-TPAT, EU의 AEO, 싱가포르의 STP 이외에도 각국에서는 세관기구를 중심으로 다양한 인증제도를 추진하고 있다. 이러한 물류보안 인증제도의 표준을 제공하기 위하여 국제표준화기구(ISO)에서는 2005년 ISO/PAS 28000 시리즈 규격을 제정하여 물류공급사슬 내에서의 물류보안경영에 대한 지침을 제공하였다. ISO 28000 인증제도의 특징은 기존의 C-TPAT, ISPS, AEO 등 다양한 물류보안인증제도를 포괄하는 개념으로 이들 물류보안인증제도와 의 적합성을 확보함으로써 ISO 28000 인증을 통하여 다른 인증제도의 직접 수용이 이루어질 수 있도록 내용이 구성되어 있다. 인증이 가능한 대상에 있어서도 공급사슬의 모든 단계에서의 제조, 서비스, 보관 또는 운송 등과 관계 있는 규모가 작은 조직에서부터 다국적 기구에 이르기까지, 모든 조직에 적용 가능하다. 이 규격은 공급사슬보안 보증에 필수적인 사항인 보안경영시스템의 수립, 실행, 유지 및 개선, 조직이 선언한 보안경영방침과의 적합성 보증, 적합성 검증, 공인된 제3자 인증기관에 의한 보안경영시스템의 인증·등록 추진 및 자체 결정 또는 선언 등을 포함한다.

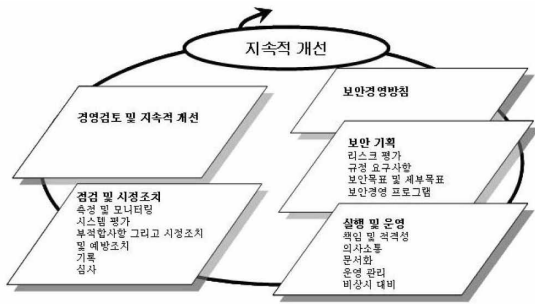


ISO 28000 시리즈 규격은 2005년 ISO/PAS(International Standard / Public Available Specification) 규격으로 WCO 등의 적극적인 지원 하에 제정되었다. 본 규격의 경우 ISO/PAS 절차를 통하여, 2년만인 2007년 국제표준화를 완료하였다. 이 시리즈 규격에는 물류공급사슬 보안경영시스템 규격에 관한 ISO 28000, 이에 대한 모범관행을 자세히 규정하고 있는 ISO 28001, 인증심사를 위한 인증기준을 제시하는 ISO 28003 및 인증제도 이행을 위한 세부 지침을 규정하고 있는 ISO 28004가 있다.



또한 지식경제부 기술표준원에서는 이러한 물류공급사슬 내에서의 보안 중요성 강화 추세에 발 맞추어, 물류보안인증제도를 도입하기 위해 2007년 KS V ISO 28000 공급사슬보안경영시스템규격 등 4종의 물류보안성명 관련 한국산업규격(KS)을 제정하였다. 7-10

물류보안경영 시리즈 규격의 주가 되고 있는 KS V ISO 28000에서는 조직의 보안경영방침에 따른 결과를 도출하는데 필요한 목표 및 프로세스를 수립하는 계획(Plan), 프로세스 실행의 실시(Do), 보안방침, 목표, 세부목표, 법규 및 그 밖의 요구사항, 그리고 보고결과에 대한 프로세스의 모니터링 및 측정을 하는 점검(Check) 그리고 보안경영시스템의 성과를 지속적으로 개선하기 위한 조치를 시행하는 조치(Act)의 4단계 P-D-C-A 사이클을 반복적으로 수행하여, 지속적으로 물류보안경영체제를 개선해 나가도록 규정하고 있다.



KS V ISO 28001에서는 공급사슬 보안 프로세스의 개발 및 실행, 공급사슬 보안 수준의 수립 및 문서화, 세계관 세기구(WCO) 규격의 SAFE framework에서 규정 한 공인 경제 운영자(Authorized Economic Operators)의 표준 제공 등 물류보안 경영의 보편 관행에 대한 요구사항 및 지침을 제공한다.

KS V ISO 28004는 KS V ISO 28000의 근본적인 원리를 설명하며, 각 요구사항의 목적, 전형적인 입력, 프로세스 및 출력에 대하여 규정하므로, KS V ISO 28000에서 규정 한 공급사슬 보안 경영시스템의 이해와 실행을 돕기 위한 것이다.

또한 KS V ISO 28000 시리즈 규격은 공급사슬 보안 경영시스템의 인증을 위한 시리즈 규격이기 때문에 공급사슬 보안 경영시스템 심사 및 인증을 제공하는 기관에 대한 원칙과 요구사항이 매우 중요하다. 이는 KS V ISO 28003에서 규정 하고 있다.

기술표준원에서는 2007년 12월 4종의 물류보안 경영 관련 한국산업규격(KS)의 도입을 완료하고, 국가표준기본법 제21조 및 한국산업표준 KS V ISO 28000에 의거 국제적으로 공인되는 물류보안 경영체제 인증기관의 인정 및 사후관리 등 인정제도를 합리적으로 시행하기 위한 세부사항을 마련하였다. 2008년 본격적인 ISO 28000 물류보안 인증제도를 추진하여 (사)한국선급을 인증기관으로 인정하였고, 부산신항만(주)은 국내 최초의 ISO 28000 인증을 획득하였다. 본 인증제도의 추진을 통하여 국가 차원에서

는 국제수준의 물류보안체계를 신속히 구축할 수 있게 되므로 물류 거점화를 촉진할 수 있는 계기를 마련하였고, 인증기업은 ISO 28000 인증 획득으로 불관심차 감소화 및 대기 시간 단축에 따른 물류비용 절감 효과를 볼 수 있을 것으로 기대한다.

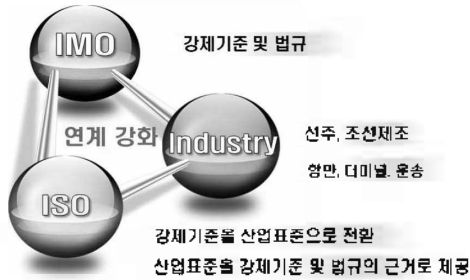
한편, 국제적으로는 2006년 9월 DP World의 두바이 본사와 Djouti 터미널이 국제최초로 ISO/PAS 28000 인증을 획득한 후, 2007년 3월에는 DP World의 뱀루머, 4월에는 도미니카공화국의 DP World Caucedo가 인증을 받았다. 미국의 경우 미국항만협회(AAPA; American Association of Port Association), 국제환경기술재단(GETF; Global Environment and Technology Foundation) 및 미국환경보호국(US Environmental Protection Agency)은 환경경영시스템(Environmental Management System)과의 협력 프로그램을 통하여 11개 항만에 대해 ISO 28000 보안경영시스템 구축을 추진하고 있다. 또한 싱가포르의 경우 국가표준화기구인 SPRING에서 표준이행 확산을 위한 프로그램을 마련하고, ISO 28000 인증 대상업체에 대한 지원을 추진하고 있다.

## 2. 해운 항만시설의 보안

IMO에서는 선주, 항만, 터미널, 운송업체 등 공급사슬 내 모든 산업계와의 연계강화 및 ISPS code 세부 상세 내용을 확보하기 위해 국제표준화기구(ISO)에서도 국제표준화를 동시에 추진하였다. ISO의 해운 및 선박 관련 기술위원회인 ISO TC8에서는 본 표준의 물류환경 변화에 미치는 중요성을 감안하여 2004년 ISO/PAS 20858 Maritime port facility security assessments and security plan development를 제정한 후, 2007년에는 ISO 20858로 국제표준화 작업을 완료하였다. 국내에도 ISPS code의 중요성과 기업들의 편의 도모를 위하여 기술표준원에서 한국산업

규격(KS)으로 2007년 11월 “KS V ISO20858 해운항만시설의 보안평가 및 보안계획서 개발”을 제정하였다. 11

국제기구 및 산업계와 연계 강화를 위한 국제표준 확보

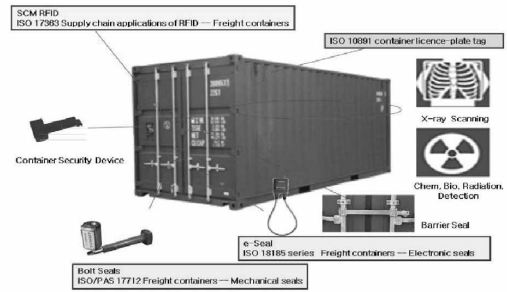


KS V ISO 20858 규격에서는 외부 심사자에 의해 검증될 수 있는 방식으로 ISPS Code에 적합함을 실증하기 위한 요구사항을 규정함 규격으로, ISPS에 의해 요구되는 보안계획서를 개발하는 인원의 적격성을 규정하고, 해운항만시설보안평가를 수행하며, 항만시설 보안계획서의 작성 및 실행이 있어서 해운항만시설에 도움을 주기 위한 기본 기준을 규정하고 있다. 또한 자격 있고 공인된 대행기관에 의하여 독립적인 검증을 허용하는 방식으로 절차를 기록하도록 규정하고 있다.

항만시설은 보안평가를 수행하여야 하며, 보안평가의 범위는 위협당할 수 있거나 해상 무역을 위협하는데 사용될 수 있는 항만시설 및 기반시설 까지 확대하여 항만시설 내에서 항만시설 및 선박 운영이 이루어지는 지역, 항만시설 내에서 화물이 해상 운송 전후에 양하, 적하 또는 처리되는 지역, 항만 시설 내에서 해상 운송을 위한 화물서류가 처리 및 접근이 용이한 지역, 보안경계선의 간섭 없이 항만시설에 추가된 지역, 그리고 항만시설에 접근하기 위해 사용되는 선박 항로를 포함한다.

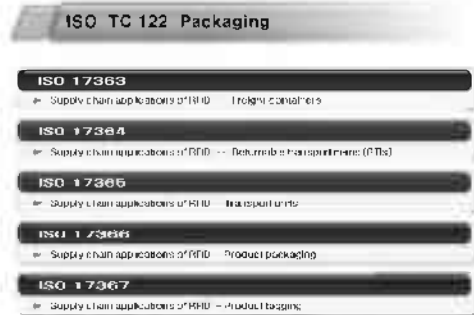
### 3. 컨테이너 관련 물류보안 기술 및 표준

해상물류가 주류를 이루고 있는 현행 국제무역에 있어서는 화물컨테이너의 보안장치가 물류보안기술의 주를 이룬다고 할 수 있다. 이와 관련된 기술로는 물류공급사슬 내의 RFID 기술, 컨테이너보안장치(CSD; Container Security Device), X선 검색, 방사능 검색, 기계적 봉인 및 전자봉인으로 크게 나누어 생각할 수 있다.

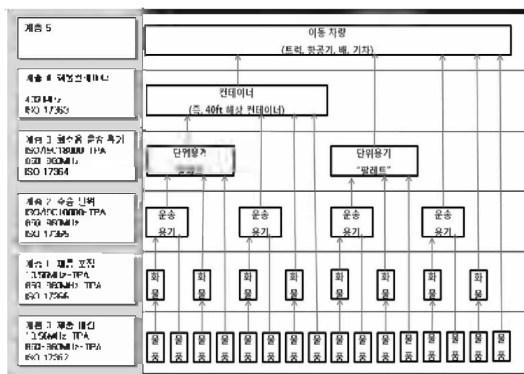


공급사슬(Supply Chain)이란 원자재로부터 판매, 사용, 유지 그리고 잠재적인 일회성 사용 그리고 회수품에 대하여 최종 목적지까지 완제품을 수송하는 모든 과정을 포함하는 다단계 계층을 가지고 있다. 각 단계에서 다루는 제품과 업무 프로세스는 다른 단계에 대하여 독립적이기도 하고 유기적으로 영향을 미치기도 하므로, 각 단계에서는 화물의 정보를 담고 있는 화물 태그의 경우 RFID 기술에 요구하는 범위가 상이할 수 있다. 따라서 국제표준화기구(ISO)에서는 ISO/TC122 포장기술위원회, ISO/TC104 화물컨테이너 기술위원회, 그리고 ISO/IEC JTC1/SC 31 데이터인식기술위원회에서 이들 관련 규격들을 참조하여 제품태깅, 제품포장, 수송단위, 회수용 운송 용기, 화물컨테이너의 계층에 따른 RFID 적용 기술에 대하여 에어 인터페이스 통신, 데이터 구조 및 데이터 요구사항을 규정하는 5개 시리즈 규격은 2007년 제정 완료하였다. 우리나라에서도 이들 규격의 한국산업규격(KS)화를 전격적으로 추진하여, 2007년 KS A ISO 17363 및 KS A ISO 17364 규격을 도

입하였고 12-13, 2008년 상반기에는 제품태깅, 제품포장, 수송단위에 관한 나머지 규격의 도입을 완료할 예정이다.



화물컨테이너의 화물정보를 담은 화물태그에 관한 KS A ISO 17363에서는 433MHz 주파수대역을 사용하며, 화물 컨테이너 공급사슬용 RFID 시스템과 그 구성요소의 실행에 대해 규정하고 있다. 또한 시행을 위해서 만족해야 할 요구사항을 기능적 요구 성능, 데이터 요구조건, 데이터 보안 요구조건, 태그 위치 요구조건, 태그 운영 요구조건 및 보안과 프라이버시 요구조건으로 구분하여 규정하고 있다. 아래 그림에서는 물류공급사슬 내에 계층에 따른 사용 주파수대역과 적용 국제표준을 제시하고 있다.

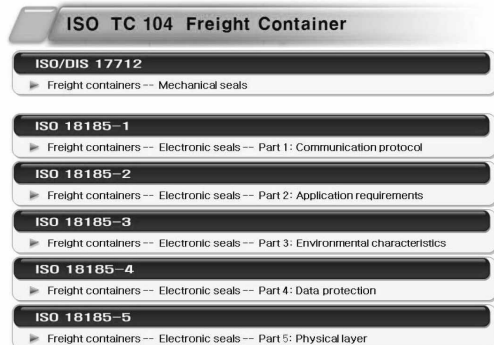


화물컨테이너를 안전하게 운송하는 대표적인 사용 보안장치인 기계적 봉인장치에 관한 국제표준인 ISO/PAS 17712:14 에서는 화물컨테이너에 대한 기계적 봉인의 분류, 수용, 철거 등의

일련에 절차에 관하여 규정한다. 따라서 본 규격에서는 봉인이 갖추어야 하는 요건으로서 사고나 환경변화에 파손되지 않을 정도로 견고하며, 통상의 사용에 있어 부정수단에 의해 파손되지 않고 사용이 용이하게 디자인 되어야 하는 기계적 봉인 요구조건, 보안 등급에 따른 I, S, H 표시 및 제조자 표시, 식별표시 및 부정사용을 방지하기 위한 중빙 등에 관한 요구조건을 규정하고 있다. 기계적 봉인에 대한 물리적인 성능 확보를 위하여 강도, 선단강도, 굽힘강도, 충격강도에 대하여 봉인의 등급에 따른 요구치를 제시하고 있다.

화물컨테이너의 전자봉인은 RFID 장치를 사용하여 기계적 봉인 장치에 화물의 자동식별이 가능한 기능을 추가하는 개념으로, 기계적 봉인보다 화물의 효율적인 운송과 화물컨테이너의 안전을 확보에 유리할 것으로 전망되어, 많은 사람들의 주목을 받고 있는 물류보안 장치이다. ISO TC104 화물컨테이너 기술위원회에서는 앞으로 입증할 것으로 예상되는 전자봉인장치의 국제적인 기준을 제정하고자 ISO 18185 시리즈 규격 5종을 2007년 제정하였다.15-19

전자봉인(e-seal)은 읽기 전용이고, 재사용이 불가능한 화물 컨테이너 봉인 장치이며, ISO 17712 기계적 봉인에 정의된 고도의 보안이 적용되는 봉인 장치 조건을 만족해야 하고, 화물의 자동 식별이 가능한 부선인식 기능을 갖추어야 한다.





전자봉인의 통신프로토콜을 규정한 ISO 18185-1 Freight containers - Electronic seals - Part 1 : Communication protocol 에서는 433MHz와 2.4GHz의 주파수 대역을 사용하는 화물 컨테이너용 전자 봉인 장치의 통신 프로토콜과 관련하여 제반 파라미터를 규정하고 태그와 호출기의 상호 운용성을 확보 할 수 있도록 국제 표준을 제정하였다. ISO 18185 규격에서는 읽기 전용의 새사용이 불가능한 화물 컨테이너 봉인 인식 체제를 규정하며, 또한 사용의 정확성을 입증하는 봉인 상태 인식 체제, 배터리 상태 지시기, 제조업체 인식을 포함하는 봉인 장치 인식기 및 봉인 태그 종류에 관해 규정하였다.

ISO 18185-2 Freight containers - Electronic seals Part 2 : Application requirements 에서는 433MHz와 2.4GHz의 주파수 대역을 사용하는 화물 컨테이너용 전자 봉인 장치의 응용 요구 조건과 관련하여 제반 파라미터를 규정하고 있다. 모든 전자봉인은 제조 시에 봉인 장치에 영구적으로 프로그램 되며, 변조 될 수 없는 봉인 장치 ID를 가지며, 봉인 장치 번호는 사용자 또는 제조업체에 의하여 할당되며, 제조업체에 의하여 프로그램되어 봉인 장치 외부(케이스)에 표시되어야 한다. 봉인 장치가 폐쇄되고, 봉인 될 때까지 봉인 장치는 응답하지 않는다. 또한 물류보안에 있어 가장 중요한 정보로 인식되고 있는 봉인 장치 태그 형식, 건진시 수명, 봉인 상태 비트, 봉인 장치 태그 제조업체 ID 및 봉인 날짜와 시간에 대해서도 규정하고 있다.

ISO 18185-3 Freight containers - Electronic seals - Part 3 : Environmental characteristics는 ISO 18185 시리즈 규격, ISO 10374(화물 컨테이너 - RF 자동 인식)와 ISO 17363(RFID의 물류 응용 - 화물 컨테이너)을 위한 환경적 요구조건을 기술한다. 환경적 요구조건으로는 저온, 고온, 기계적 충격, 랜덤한 진동, 습도, 비·눈, 염분성 안개, 낙하충격, 모래와 먼지 및 전기적 환경에 대한 요구조건이 있다.

ISO 18185-4 Freight containers - Electronic seals- Data protection 규격은 봉인장치 및 이와 연관된 리더간의 통신과 관련한 데이터 보호, 장치 인증, 전자 봉인장치의 적합성에 대한 요구사항에 대하여 규정한다. 적합성에 대한 요구사항은 접근성, 비밀성, 데이터부실성, 인증, 저장된 데이터에 대한 변조방지에 관한 내용을 포함한다.

ISO 18185-5 Freight containers- Electronic seals Part5: Physical layer에서는 컨테이너 전자 봉인장치의 리더 및 호출기간의 에어 인터페이스에 대해 규정한다. 시스템은 전자 봉인장치, 저주파 송신기와 리더기 등의 세 요소로 구성되어, 두 개의 주파수를 이용하는 이중 주파수 동작(Dual Frequency operation) 형식을 따르고 있다. A 타입의 물리 계층은 433MHz의 장거리 링크와 OOK 저주파 단거리 링크를, B타입의 물리 계층은 2.4GHz의 장거리 링크와 PSK 단거리 링크로 전자 봉인장치는 두 종류의 에어 인터페이스를 지원해야 한다.

이상에서 살펴본 바와 같이 전자봉인 장치는 433MHz와 2.4GHz의 두 가지 주파수대를 사용하여 주파수대가 다른 모든 국가에서의 통신이 가능하고 저주파 근거리 통신으로 컨테이너의 위치를 파악할 수 있다는 장점이 있다. 그러나 전자봉인은 컨테이너의 화물정보와 같은 주요 정보를 가지고 있지 않기 때문에 데이터 보호 기술을 적용하고 있지 않은 것은 취약점으로 지적되고 있다. 따라서 국제표준과는 상이하지만 여러 가지 기능을 가지는 전자봉인장치에 대한 개발도 이루어지고 있다. GE, 지멘스, 미쓰비시 그리고 삼성물산이 공동으로 상용화를 추진하고 있는 컨테이너보안장치가 대표적인 예로서, 기능면에서 살펴보면, 통신 주파수대역을 2.4GHz으로 설정하고, ISO 18185에서 규정하고 있는 전자봉인, 컨테이너 태그 및 화물 태그의 기능을 제공하고 이외에도 화물정보, 공급사슬 관리정보 및 컨테이너 이동상황에 관한 데이

터블 부가적으로 제공하고 있다. 또한 보안장치를 키체이너 내부에 설치하도록 함으로 해상환경에 대한 내구성을 확보하여 재사용이 가능하도록 설계되어 있다. 데이터보호 측면에 있어서도 Kerberos 네트워크 인증서비스와 AES-128 데이터 암호화 기법을 사용함으로써 데이터 보호를 강화하고 있다.

### III. 물류보안에 대한 대처방안

최근 글로벌 물류보안체제 구축 동향은 정부-정부, 정부-민간기관, 민간기관-민간기관의 상호협력 관계들을 강조하며 전개되고 있다. 따라서 국제적으로 모든 나라에서는 물류보안에 있어서 정부의 역할만을 강조하는 것이 아니라, 정부와 민간기관과의 역할에 대한 효율적인 관계 설정에 노력하고 있다.

우리나라에서도 정부-정부간 상호협력을 위한 국가 물류보안체제 기반구축을 위하여 국토해양부에서는 항공안전 및 보안에 관한 법률 및 국제 항해선박 및 항만시설의 보안에 관한 법률을 운영하고 있으며, 관세청은 AEO 물류보안인증제도를 위한 관세법을 개정하는 등 각 물류 관련 부처를 중심으로 다양한 입법화가 추진되고 있다.

또한 정부와 민간기관과의 협력 강화를 위하여 국가정보원을 주축으로 지식경제부, 국토해양부, 외교통상부, 관세청 등 관련 정부 부처 및 무역협회, (사)한국선급, 한국해양수산개발원 등 관련 기관, CSD 업체인 삼성물산, X선 검색기 개발업체인 이비테크 등 민간업체가 함께 하는 민관협의체를 운영하며, 글로벌 물류보안 환경변화에 대한 정확한 정보 교환 및 각 분야의 물류보안체제 통합조정을 위해 노력하고 있다. 이러한 정부-민간간의 상호협력이 가시적인 성과를 거두기 위해서는 무엇보다 물류보안 정책을 주도하고 있는 관련 기관들이 글로벌 물류보

안 환경변화를 정확하게 인식하고, 이에 대한 적절한 통합조정에 노력을 기울여야 한다. 또한 글로벌 물류보안 환경은 미국을 중심으로 한 정책의 변화에 민감하게 반응하므로, 수동적인 수용 자세에서 한 걸음 나아가 DP World의 ISO 28000 인증이나 싱가포르의 STP와 같이 신속한 대응 방안 마련에 의한 경쟁력 선점 효과를 추구하여야 할 것이다.

민관기관 간의 물류보안협력에 있어서는 물류업계의 인식 부족 및 시스템 제공 업체의 부재 등에 기인하여 가시적인 성과를 찾아 볼 수 없는 형편으로, 우리나라 물류보안에 있어 가장 미진한 분야라고 할 수 있다. 우선 민간업체의 올바른 물류보안 의식 고취를 위하여 관련 기관에서는 세미나, 교육, 훈련 등의 다양한 홍보 프로그램을 개발하는 것이 시급하다. 이를 통하여 물류업체들은 기회 비용을 줄일 수 있으며, 민간-민간 상호협력의 기반도 확보할 수 있을 것으로 기대한다. 따라서 정부 기관에서는 정부간 상호협력을 위한 물류보안체제 구축보다 민간 물류업체가 물류보안경영체제를 갖추 수 있도록 노력하여야 할 것이다.

글로벌 물류보안 환경변화는 미국 등 주요 국가를 중심으로 자국의 물류보안 체제를 강화하고, 국제표준을 신장하며, 자국 내 장비산업체를 지원하는 방향으로 다소 국제 무역 질서에 반하는 방향으로 진행되고 있는 것을 간과할 수 없다. 또한 물류보안인증제도 등 상호협력 프로그램 개발을 통하여 신속한 물류보안 정보 교환을 강제화하고 있어, 이를 위한 선진 장비 설치 및 활용이 불가피한 실정이다. 또한 가장 두드러진 특징 중에 하나는 제도의 취시가 상호협력력을 통한 물류보안 확보 및 국제 교역의 원활화라고 하더라도 미국 등 주요국가가 주도하는 물류보안체제 구축에 협력해야 하는 실정이다.



그러므로 국가물류보안체제 구축을 통한 물류 경쟁력 향상을 도모하고자 하는 우리 입장에서는 글로벌 물류보안 환경변화 및 기술 변화에 신속하게 대응하여, 신진 물류보안 기반을 하루 속히 갖추는 것이 급선부이다. 또한 시스템 기술의 종속으로 인한 불이익을 최소화하기 위하여 물류보안 산업의 육성 및 지원에도 그 노력을 아끼지 말아야 하겠다.

#### 참고문헌

1. <http://homeport.uscg.mil>
2. [http://www.ep.gov/xp/cgov/mportico/mmercia\\_enforcement/ctctst/](http://www.ep.gov/xp/cgov/mportico/mmercia_enforcement/ctctst/)
3. [http://www.ep.gov/xp/cgov/border\\_security/international\\_activities/](http://www.ep.gov/xp/cgov/border_security/international_activities/)
4. [http://www.cbp.gov/xp/CustomsToday/2007/apr\\_may/secure.xml](http://www.cbp.gov/xp/CustomsToday/2007/apr_may/secure.xml)
5. [http://www.mo.org/Newsroom/mainframe.aspx?topic\\_d=897](http://www.mo.org/Newsroom/mainframe.aspx?topic_d=897)
6. <http://www.wcoomd.org/speeches/default.aspx?c=1&d=5/>
7. KS V ISO 28000 공급사슬 보안경영시스템 규격
8. KS V ISO 28001 공급사슬 보안경영시스템-공급사슬의 보안, 평가 및 계획의 실행을 위한 모범관행 - 요구사항 및 지침
9. KS V ISO 28003 공급사슬 보안경영시스템-공급사슬 보안경영시스템 심사 및 인증을 제공하는 기관에 대한 요구사항
10. KS V ISO 28004 공급사슬 보안경영시스템 - KS V ISO 28000 실행지침
11. KS V ISO20858 해운 항만시설의 보안평가 및 보안계획서 개발
12. KS A ISO 17363 무선인식(RFID)의 공급망 응용-화물 컨테이너
13. KS A ISO 17364 무선인식(RFID)의 공급망 응용-회수용 운송 용기
14. ISO/PAS 17712 Freight containers-Mechanical seals
15. KSAISO18185-1 화물 컨테이너-전자 봉인장치- 제1부:통신 프로토콜
16. KSAISO18185-2 화물 컨테이너-전자 봉인장치- 제2부:응용 필요조건
17. KSAISO18185-3 화물 컨테이너-전자 봉인장치- 제3부:환경 특성
18. KSAISO18185-4 화물 컨테이너-전자 봉인장치- 제4부:데이터 보호
19. KSAISO18185-5 화물 컨테이너-전자 봉인장치- 제5부:물리 계층

기술표준 2008.7