經營學碩士 學位論文

ISPS Code에 規定된 港灣施設 保安評價를 施行하기 위한 方法論에 關한 硏究

A Study on the Methodology for Undertaking the Port Facility Security Assessment of the ISPS Code

指導敎授 金 吉 洙

2004年 12月

韓國海洋大學校 大學院

海運經營學科 金 濠 均

< 목 차 >

< 표 목 차 >

< 그 림 목 차 >

Abstract

A Study on the Methodology for Undertaking the Port Facility Security Assessment of the ISPS Code

Kim, Young-Kyoon
Department of Shipping Management
Graduate School of Korea Maritime University

It has been identified through this study that a security assessment which is undertaken in advance of establishing a port facility security system should be performed correctly in order to ensure that the system is set up in accordance with the ISPS Code. Also it was found that an appropriate methodology is required to undertake the port facility security assessment in a correct manner.

The risk assessment methodology applied in the safety fields has been adopted as the methodology for the security assessment for this study. This study looks at seven stages of risk assessment.

At first stage, the identification and evaluation of important assets and infrastructure requiring protection is carried out. Such undertakings are needed to clearly identify the function of the assets and infrastructure within the port facility, ascertain ones that are to be protected from

security threats or security incidents, decide on their relative importance, and determine which ones are to be subjected to the security assessment. All identified assets and infrastructure should be included in the evaluation. Three parts should be considered in the evaluation. First, the role or objective of the assets and infrastructure in the operation of the port facility should be considered. The next consideration should be the effect of destruction. Finally, the ability to recover from destruction of the assets and infrastructure should be considered.

At second stage, an on-site security survey is carried out. An on-site security survey is a process through which the present security conditions of the port facility and of the important assets and infrastructure within port facility can be identified. When conducting such on-site security survey, security procedures, security organizations, security equipments and systems, and the security ability of the port facility personnel having specific security duty should be considered.

At third stage, the identification of the possible threat scenarios and security incidents to the important assets and infrastructure is carried out. The security incidents that had occurred in the past and the security rule or regulations for the security in force should be considered at the time of identifying the security threats and incidents. And the consultation with the security expert authority should also be carried out.

At fourth stage, the assessment of consequence and vulnerability is carried out. The consequence and vulnerability should be evaluated to confirm the effect of identified security incident and the probability of the target to the attack. Five elements are included in the consequence assessment: death and injury, economic impact, environmental impact, national defense impact, and symbolic effect. And the vulnerability assessment should be evaluated in two parts: accessibility and organic security. The results of the on-site security survey carried out at the second stage should be considered in the vulnerability assessment.

At fifth stage, the security risk level is determined. The security risk level should be determined based on the level of consequences and vulnerability. The security risk is classified into three levels: mitigate, consider and document.

"Mitigate" means that mitigation strategies should be developed to reduce risk for that threat scenario.

"Consider" means that the threat scenario should be considered and mitigation strategies should be developed on a case-by-case basis.

"Document" means that the threat scenario does not need a mitigation measure at this time and therefore need only to be documented.

At sixth stage, the mitigation targets and implementation methods is determined. The mitigation targets should be identified based on the security risk level. And the mitigation methods to be implemented for that target should be decided based on the effectiveness and possibility of the methods. Generally, it is required to consider the mitigation strategies in lowering vulnerabilities in advance than the mitigation strategies in lowering consequences.

At seventh stage, the security risk reassessment is carried out. And the confirmation of mitigation measures is carried out based on the result of the reassessment. A security risk reassessment to the mitigation measures determined at the sixth stage should be practiced to confirm whether the measures can actually reduce the security risk level. The reassessment should be started from the fourth stage. If the security risk level is not reduced as the result of the reassessment, another mitigation measures should be considered for implementation. If the security risk is reduced as the result of the reassessment, the mitigation measures should be adopted and planned to be put into action in the port facility security system.

제1장 서론

제1절 연구의 배경

2001년 9월 11일 미국에서 발생한 항공기 테러(이하 9.11 테러라고 함) 사건은 테러 방법의 대담성과 엄청난 피해로 인하여 전 세계에 크나 큰 충격을 주었다. 그 충격으로 테러 위협에 대한 경각심이 고조되었고 다방면에 걸쳐 테러에 대한 대비책 마련의 필요성을 느끼게 되었다.

9.11 테러가 그 이전의 테러와 다른 것은 비행기 자체를 무기로 사용하여 테러를 시도하였다는 점이다. 이전의 테러는 비행기를 납치하거나 폭발시키고, 인질을 납치하거나 주요 시설을 파괴하는 것으로 자신들의 목적을 달성하려고 하였다. 그러나 9.11 테러는 비행기를 납치하고, 납치한 비행기를 무기로 사용하여 많은 수의 인원들이 상주하는 건물을 파괴함으로써 엄청난 피해를 야기하였다. 이는 이전의 테러 방법과는 확연히 다른 것으로서 극도의 공포감을 유발시켰고 언제든지 다시 이런 엄청난 테러가 발생할 수도 있다는 불안감을 가지게 하였다.

이러한 특징을 가진 테러는 해상 수송 분야에서도 그대로 발생할 수 있을 것이다. 특정 항구에서 대형 유조선이나 LNG 선박 같은 특수 선박을 납치하여 폭파를 시도한다면 항구의 기능이 마비되는 것은 물론 항구 인근 지역에 엄청난 피해를 초래할 수 있고 그로 인한 심리적 충격은 상당할 것이다. 또한 대형 여객선에 대한 폭파를 시도한다면 엄청난 인명 피해를 초래할 수도 있을 것이다.

국제해사기구(IMO)에서는 이러한 테러 위협에 체계적으로 대응하고자 1974년 해상인명안전협약(International convention for the safety of life at sea, 1974 SOLAS. 이하 SOLAS라고 함)에 제11-2장[1] 해상보안 강화를 위한 특별조치를 신설하였다. 또한 선박 및 항만시설(port facility)[2]이 보안시스템을 수립하는데 필요한 기준을 제정하여 국제 선박 및 항만시설 보안규칙(International code for the security of ships and of port facilities, ISPS Code)으로 공표하였다. 그리고 SOLAS 제11-2장에서 해상보안을 위한 강제

1) 기존의 제11장을 제11-1장으로 하고, 해상보안 강화를 위한 특별조치를 제11-2장으로 별도의 장을 구성하였다.

2) SOLAS 제11-2장의 정의에서는 항만시설(port facility)을 다음과 같이 정의하고 있다. “선박/항만 인터페이스가 발생하는 장소. 여기에는 묘박지(anchorage), 대기선석(waiting berth) 및 해상으로부터의 진입수역(approaches from seaward) 등도 포함됨.”

규칙으로 ISPS Code를 시행하도록 하는 근거 규정을 마련하였다.

SOLAS 제11-2장의 관련 규정에 따라 2004년 7월 1일부터 전 세계적으로 발효된 ISPS Code는 국제항해에 종사하는 SOLAS 적용 대상선박 및 이들 선박과 인터페이스[3]가 발생하는 항만시설들이 ISPS Code에서 규정하고 있는 요건에 적합한 보안시스템을 수립할 것을 요구하고 있다. 그리고 만약 ISPS Code에 따른 보안시스템을 수립하지 못한 경우에는 선박 운항 및 항만시설 운영에 불이익을 받을 수 있다.

SOLAS 제11-2장 및 ISPS Code에서 우리가 주목해야 할 사항 중의 하나는 그 적용 대상이 국제항해에 종사하는 선박뿐만 아니라 이들 선박과 상호교류 작용이 발생하는 항만시설도 포함된다는 것이다. 지금까지의 SOLAS 협약의 모든 조항은 선박에만 적용되는 것이었다.

그러나 해상 보안이 확보되기 위해서는 선박뿐만 아니라 항만시설에서도 보안시스템이 구축되어야 한다. 그러므로 IMO에서는 지금까지 선박에만 적용되던 SOLAS 협약의 적용 범위를 항만시설에까지 확대하여 적용하기로 결정하고 ISPS Code를 제정하면서 적용 범위를 SOLAS 협약 대상 선박이 사용하는 항만시설을 포함시켰다.[4] 따라서 SOLAS 적용 대상선박과 인터페이스가 발생하는 항만시설에서는 ISPS Code에 따른 보안시스템을 수립하여 시행하고 그 사항을 IMO에 통보하여 당해 항만시설이 ISPS Code에 따른 보안시스템을 수립하여 적용하고 있는 항만시설임을 명확히 나타내어야 한다. 만약 그렇지 못한 경우에는 당해 항구에 입항하였다가 오는 선박에 대하여 다른 항구에서 불이익을 줄 수 있으므로 선박 운항자들은 그런 항만시설에 입항하기를 주저할 것이다.

또한 미국은 ISPS Code를 근거로 자국법인 해상교통보안법(Maritime Transportation Security Act, MTSA 2002)을 제정하면서 미국과 교역이 있는 외국항만의 보안시스템이 ISPS Code에 따라 적절히 유지되고 있는지를 평가하는 조항을 MTSA에 규정하였다. 그리고 평가 결과 보안시스템 유지 상태가 만족하지 못한 항만에 대해서는 일정기간 동안 유예기간을 주고 만족한 수준

---

3) SOLAS 제11-2장의 정의에서는 선박/항만 인터페이스(ship/port interface)를 다음과 같이 정의하고 있다. "인원, 화물의 이동 또는 선박에 대하여 또는 선박으로부터의 항만 서비스의 제공을 포함한 활동이 선박에 직·간접적으로 영향을 미칠 때 야기되는 상호작용"

4) ISPS Code A편 서문에서는 SOLAS를 항만시설에 적용하는 이유는 SOLAS가 필요한 보안조치의 발효 및 신속한 효과를 얻을 수 있는 가장 빠른 수단을 제공한다는데 근거하여 동의되었다라고 규정하고 있다. 그러나 너무 확대하여 적용하는 것을 방지하기 위하여 항만시설에 관련되는 규정은 선박/항만 인터페이스 사항에만 국한되어야 한다고 규정하고 있다.

에 이르도록 하며 그래도 만족스럽지 못한 경우에는 불이익을 주도록 규정하고 있다.[5)]

지금까지는 항만운영에 대하여 국제협약이 강제적으로 적용되는 일이 없었다. 그러나 해상교통에 대한 보안 문제에 있어서는 항만 및 항만시설들이 매우 주요한 대상이 되고 있으며 그 결과 국제협약이 직접적으로 적용되는 대상이 되었고, 미국과 교역이 있는 국가들 같은 경우에는 자국의 항만 보안시스템이 미국의 평가결과 만족스럽지 못하면 미국과의 교역에도 직접적으로 큰 영향을 미치므로 자국 항만이 보안상으로 안전하다는 신뢰를 줄 수 있도록 하는 것이 무엇보다도 중요하게 되었다.

해양선진국으로 발전해가고 있고 IMO 내에서도 선두 그룹으로 도약하고 있으며 또한 대외 교역국가 중에서 가장 의존도가 높은 무역상대국인 미국과 무역을 하고 있는 우리나라는 SOLAS 제11-2장 및 ISPS Code를 명확히 이해하고 ISPS Code에 적합한 보안시스템을 수립하여 유지하는 것이 우리나라 항만에 입항하는 선박에 불이익을 주지 않을 것이며 또한 우리의 수출에도 나쁜 영향을 미치지 않을 것이다.

이러한 국제적인 환경의 변화에 대응하고자 본 연구는 국내의 항만시설들이 ISPS Code에 따른 보안시스템을 수립하고자 할 때 반드시 선행되어야 하며 또한 항만시설의 보안시스템 수립에 가장 중요한 부분이라고 할 수 있는 항만시설 보안평가에 대한 방법론을 제시하여 보고자 한다.

---

5) MTSA 2002, Section 1, Title I-해상운송보안, Sec.102 "항만보안"에 외국항만의 평가와 관련된 사항을 규정하여 두고 있으며 다음과 같은 내용이 주요 골자이다.
(1) 70108항에서는 국토보안부(Department of Homeland Security) 장관은 미국으로 향하는 선박들이 출발하는 외국항만, 그리고 장관이 국제해사무역에 보안위협을 가한다고 믿는 기타 항만에서 이행되는 대테러조치의 효과성을 평가하여야 한다고 규정되어 있음. 효과성 평가의 대상에는 1) 컨테이너로 된 것, 기타 화물이나 짐의 검색 2) 화물, 선박 및 부두 측 시설물에 대한 접근제한수단 3) 추가의 선박 보안 4) 적절한 보안표준에 대한 적합증서 또는 면허 5) 외국 항에 대한 보안관리 프로그램 6) 미국에 대한 테러를 저지하는 다른 적절한 수단 등이 규정되어 있음.
(2) 70109항에서는 평가 결과 효과적인 대테러조치를 이행하지 못한 경우에 국토보안부 장관은 발견된 사실을 해당정부에 통보하고 대테러조치를 증진시키기 위해 필요한 단계를 요청하도록 규정하고 있음.
(3) 70110항에서는 70109항에 따라 통보 후 90일 이후에도 대응조치를 취하지 못한 경우에는 통보 후 90일 이후부터 적절한 제재 조치를 시행할 수 있다고 규정하고 있음. 제재조치에는 해당 항만으로부터 출발한 선박에 대한 입항 거부 조치도 포함되어 있음.

제2절 연구의 목적

SOLAS 제11-2장에는 항만시설은 ISPS Code B편에 주어진 지침을 고려하여 ISPS Code A편의 관련 요건들에 적합하여야 한다고 규정되어 있다. 또한 항만시설보안평가(port facility security assessments)를 시행하여야 하며 항만시설보안계획서(port facility security plan)를 개발하도록 요구하고 있다.[6] 즉 다시 말하면 항만시설은 ISPS Code A, B편의 요건들을 반영한 보안시스템을 수립하여야 되는 것이다.

항만시설이 ISPS Code에 따른 보안시스템을 수립하기 위해서는 ISPS Code에 대한 정확한 이해가 선행되어야 한다. 즉 ISPS Code를 정확히 이해하여야만 당해 항만시설에 효과적이고 적절한 보안시스템을 수립할 수 있다. 또한 항만시설이 효과적이고 적절한 보안시스템을 수립하기 위해서는 체계적인 접근이 필요하다. ISPS Code에는 항만시설이 보안시스템을 수립할 때 요구되는 기본적인 사항이 규정되어 있다. 그러나 이 기본적인 사항을 구체적으로 시행하기 위한 방법은 규정되어 있지 않다. 항만시설보안평가의 경우에도 항만시설보안평가에 포함되어야 하는 최소한의 사항은 규정되어 있지만 항만시설보안평가를 시행하기 위한 방법에 대해서는 어떤 사항도 언급되고 있지 않다.

이에 본 연구에서는 항만시설보안평가를 시행하기 위한 방법론을 정립하기 위하여 안전 분야의 위험성평가 방법론을 분석 조명하여 보고 연관 관계를 분석하여 항만시설보안평가에 적용하기 위한 실제적인 방안을 모색하고자 한다.

이런 관점에서 본 연구의 목적을 구체적으로 서술하면 다음과 같다.

첫째, ISPS Code의 내용을 조명하여 항만시설 보안시스템과 연관된 요건을 파악하고자 한다.

둘째, 항만시설 보안평가의 방법론을 구축하기 위하여 안전 분야에서 적용하는 위험성평가 방법론을 종합적으로 고찰하고 항만시설 보안평가에 적용하기 위한 이론적 방안을 모색하고자 한다.

셋째, 위험성평가를 근거로 수립한 이론적 방안을 토대로 항만시설 보안평가 방법론을 정립한다.

넷째, 항만시설 보안평가 방법론을 바탕으로 현실적으로 항만시설들이 적용할 수 있는 항만시설 보안평가 방안을 제시하고자 한다.

---

6) SOLAS 제11-2장, 제10규칙, 1항 및 2항에 규정되어 있다.

제3절 연구의 방법 및 구성

본 연구는 항만시설 보안평가에 대한 방법론을 찾아서 보안평가를 시행하기 위한 구체적인 방안을 수립하기 위해 국내외 문헌고찰에 의한 이론적 연구와 분석을 병행하였다. 먼저 안전 분야의 위험성평가 방법을 종합적으로 고찰하여 항만시설 보안평가를 시행하기 위한 모델을 설정하였다. 다음으로 설정된 모델을 기준으로 현실적으로 적용하기 위한 방안을 설정하기 위하여 미 해안경비대(USCG)의 지침, 국제표준화기구(ISO)의 지침 및 IMO/ILO 공동 지침 등을 참조하였다.

본 연구의 구성은 다음과 같이 다섯 개 장으로 구성되어 있으며 각 장의 주제에 필요한 모든 사항을 연구범위로 한다.

제1장은 연구를 수행하게 된 목적과 범위를 기술하였다. 제2장은 ISPS Code의 제정 배경과 채택경위 및 그 내용을 분석하였다. 제3장은 항만시설 보안평가를 하는 방법론의 모델이 되는 위험성 평가에 대하여 구체적으로 조명하고, 위험성 평가를 근거로 항만시설 보안평가의 모델을 구성하였다. 제4장은 항만시설 보안평가 모델을 근거로 항만시설 보안평가를 하기 위한 구체적인 방안을 수립하였으며 그 방안을 실제 적용하여 모델의 실효성을 검증하였다. 마지막으로 제5장은 이 연구의 결론으로 연구 결과의 요약과 이 연구가 갖는 한계와 향후 연구 과제를 기술하였다.

제2장 ISPS Code의 제정 및 내용에 대한 분석

본 장에서는 SOLAS 제11-2장 및 ISPS Code가 제정되고 SOLAS에 채택된 배경 및 경과 과정을 정리하고 그 내용을 분석하였다. 그리고 ISPS Code에 따른 보안시스템의 인증 제도를 아울러 고찰하였다. 이로써 본 연구의 연구대상인 항만의 보안시스템을 보다 명확히 인식하고 항만의 보안시스템을 수립하기 위해서 필요한 구성 요소들을 구체적으로 조명하고자 한다.

제1절 ISPS Code 제정 배경

9.11 테러는 전 세계에 테러의 공포감과 함께 테러 위협에 대한 경각심을 일으켰으며 이로 인하여 테러에 대한 대비책이 필요하다는 것을 인식하는 계기가 되었다.

9.11 테러 이후 국제해사기구(IMO)에서는 9.11 테러와 같은 형태의 테러가 해상에서도 일어날 수 있다는 점을 인식하였다. 그래서 해상에서의 테러를 예방하기 위한 수단이 필요하다는 점에 모든 협약 당사국들이 공감하였다. 또한 국제해사기구는 해상에서의 테러를 방지하기 위해서는 선박뿐만 아니라 항만도 테러를 방지하기 위한 체제를 갖추어야 하며, 선박과 항만이 서로 협력하는 가운데 해상 수송 분야에서의 보안 위협이 예방될 수 있다는 것을 인식하였다.

그리고 국제해사기구는 협약 당사국들이 해상에서의 테러를 방지하기 위한 보안시스템을 수립하고 시행하기 위해서는 국제적으로 통일된 기준 및 지침을 제공할 필요성이 있음을 인식하였다. 또한 협약 당사국들이 이러한 보안시스템을 지속적으로 유효하게 시행하도록 하기 위해서는 국제협약에 이를 반영하여 강제적인 시행을 할 필요가 있음을 인식하였다.

제2절 ISPS Code의 채택 및 SOLAS 협약에 반영된 과정

2001년 11월 개최된 국제해사기구(IMO) 제22차 총회에서 “승객, 선원 및 선박의 안전을 위협하는 테러행위 방지대책 및 절차의 검토에 관한 결의서”[7]를 채택하였다. 또한 선박 및 항만시설의 보안에 관한 새로운 조치의 개발을 채택하기 위하여 1974년 해상인명안전협약의 당사국간 회의(해상보안에 관한 외교회의)를 2002년 12월에 개최하는 것에 만장일치로 동의하였다.

---

7) IMO Res. A. 924(22).

2001년 11월에 개최된 해사안전위원회 제1차 임시회기에서 적절한 보안 조치의 개발과 채택을 가속화시키기 위하여 해상보안에 관한 해사안전위원회(Maritime Safety Committee, MSC)의 회기간 작업반(Intersessional Working Group, ISWG)을 구성하였다.

2002년 2월 개최된 회기간 작업반(ISWG) 1차 회의에서 해상인명안전협약(SOLAS) 제5장 및 제11장의 개정안 및 ISPS Code A편 초안을 작성하였다. 제11장은 11-1장과 11-2장으로 분리하여 구성하였으며 기존의 11장은 11-1장으로 하고 해상보안에 관한 사항을 11-2장으로 신설하였다.

2002년 5월 개최된 제75차 해사안전위원회(MSC)에서 회기간 작업반(ISWG) 1차 회의에서 작성된 개정안 및 초안을 검토하였다.

2002년 9월 개최된 회기간 작업반(ISWG) 2차 회의에서 해상인명안전협약(SOLAS) 개정안 및 ISPS Code A편 초안을 재검토하였고 ISPS Code B편 초안을 작성하였다.

2002년 12월 개최된 제76차 해사안전위원회(MSC)에서 회기간 작업반(ISWG) 2차 회의의 결과물을 검토하였다.

2002년 12월 개최된 해상보안에 관한 외교회의(The Diplomatic Conference on Maritime Security)에서 해상인명안전협약(SOLAS)의 개정사항 및 ISPS Code A편 및 B편을 채택하였다.

2004년 7월 1일 해상인명안전협약(SOLAS) 개정사항 및 ISPS Code는 국제적으로 발효되었다.

제3절 ISPS Code의 신속한 채택 및 발효가 가지는 의미

일반적으로 해상인명안전협약이 개정되거나 새로운 국제규칙이 해상인명안전협약에 반영되는 경우에는 채택에서부터 발효되기 까지 약 3년 내지 5년의 준비기간을 두었다.[8] 그러나 ISPS Code는 채택에서부터 발효까지 1년 6개월이라는 극히 짧은 기간이 소요되었다. 또 필요성을 인식하고 논의를 시작한 시점부터 발효되기까지를 보더라고 2년 6개월이라는 기간밖에 소요되지 않았다.

그리고 채택을 하기위한 의결 방법에 있어서도 일반적인 절차를 거치지 않았다. 일반적으로 새로운 규칙이 발효되기 위해서는 국제해사기구의 총회의 의결을 거쳐야 하나 이번의 경우에는 2년에 한 번씩 개최되는 총회까지 기다리지 않고 협약 당사국 간의 외교회의를 통하여 채택을 하였다. 이러한 예는

8) ISM Code의 경우에는 1994년 채택되어 1998. 7. 1.에 1차적으로 발효되었으며, 2002. 7. 1.에 최종적으로 전 선종에 대하여 발효되었다.

극히 이례적인 일이라고 할 수 있다.

ISPS Code의 채택 및 발효가 이렇게 신속하게 진행된 것은 미국이 강력하게 주도하여 추진한데도 이유가 있지만 국제해사기구(IMO)의 모든 협약 당사국들이 9.11 테러로 인한 테러 피해의 심각성을 깊이 인식하고 테러 대비를 위한 국제적인 기준이 필요하다는 것을 절실하게 느꼈다고 볼 수 있다.

국제해사기구(IMO)가 해상운송분야에서의 테러를 방지하기 위하여 SOLAS 제11-2장 및 ISPS Code의 조속한 발효를 결정하였으나 채택부터 발효까지의 기간이 1년 6개월 밖에 안 되는 짧은 기간이기 때문에 시행하는데 필요한 여러 가지 사항에 대한 준비 부족이 나타날 수밖에 없었다. 그런 사항들 중의 대표적인 것은 해상보안과 관련하여 선원들이 받아야 하는 교육 및 훈련에 관한 사항이 1978 선원의 훈련·자격증명 및 당직근무의 기준에 관한 국제협약(STCW 1978 협약)에 반영되어 있지 않은 것이다.

제4절 SOLAS 제11-2장의 구성 및 내용

1. SOLAS 제11-2장의 구성

SOLAS 제11-2장은 해상보안에 대한 당사국 정부, 선박, 회사 및 항만시설의 책임 및 의무사항에 대하여 규정하고 있다. 또한 ISPS Code가 강제적으로 시행되도록 하기 위한 근거를 규정하고 있다. SOLAS 제11-2장은 전부 13개의 규칙으로 구성되어 있으며 각 규칙의 제목은 다음과 같다(<표 2-1> 참조).

<표 2-1> SOLAS 제11-2장의 각 규칙

규칙 번호	규 칙 제 목
1	- 정의(Definitions)
2	- 적용(Application)
3	- 보안과 관련한 당사국 정부의 의무사항(Obligations of Contracting Governments with respect to maritime security)
4	- 선박 및 회사의 요건(Requirements for Company and ships)
5	- 회사의 구체적 책임사항(Specific responsibility of Companies)
6	- 선박보안경보시스템(Ship security alert system)
7	- 선박에의 위협(Threats to ships)
8	- 선박의 안전 및 보안을 위한 선장의 재량권(Master's discretion for ship safety and security)
9	- 통제 및 적합조치(Control and compliance measures)
10	- 항만시설 요건(Requirements for port facilities)
11	- 대체보안협정문(Alternative security agreements)
12	- 동등한 보안 합의(Equivalent security arrangements)
13	- 정보의 통보(Communication of information)

2. SOLAS 제11-2장 각 규칙의 내용 요약

1) 정의(제1규칙)

SOLAS 11-2장 및 ISPS Code가 적용되는 용어에 대한 정의를 하고 있다. 선박의 종류 및 회사에 관한 정의는 기존 SOLAS 협약에 정의된 내용을 동일하게 적용하고 있다. 나머지 선박과 항만의 인터페이스, 항만시설, 국제 선박 및 항만시설의 보안규칙(ISPS Code), 보안사건, 보안등급, 보안선언서, 보안인증심사대행기관 등에 관한 용어를 설명하고 있다.

(1) 선박과 항만의 인터페이스(Ship/port interface) : 인원, 화물의 이동 또는 선박에 대하여 또는 선박으로부터의 항만 서비스의 제공을 포함한 활동이 선박에 직·간접적으로 영향을 미칠 때 야기되는 상호작용(1.8항).

(2) 항만시설(Port facility) : 당사국 정부 또는 지정당국이 결정한 선박/항만간 상호 작용이 발생하는 장소. 묘박지, 대기선석 및 해상으로부터의 진입수역을 포함(1.9항).

(3) 선박 대 선박 활동(Ship to ship activity) : 한 선박으로부터 다른 선

박으로의 화물 또는 인원의 이동을 포함한 항만 시설과 관련이 없는 활동(1.10항).

(4) 보안사건(Security incident) : 선박 또는 항만시설 또는 선박/항만 인터페이스 또는 선박 대 선박 활동의 보안을 위협하는 의혹행위 또는 상황(1.13항).

(5) 보안등급(Security level) : 보안사건이 시도되거나 발생할 수 있는 위험의 정도를 정한 것(1.14항).

(6) 보안선언서(Declaration of security) : 각 주체가 실행하는 보안조치의 구체적 상호작용에 관한 선박과 항만시설 또는 다른 선박간의 합의문을 말함(1.15항).

(7) 보안인증심사대행기관(Recognized security organization) : ISPS Code A편에 의해 요구되어지는 평가, 심사, 승인 또는 증서발급업무의 수행권한이 있고 보안문제에 있어 적절한 전문기술이 있으며 선박 및 항만운용에 대한 적절한 지식을 지닌 기관(1.16항).

2) 적용(제2규칙)

해상보안을 위한 특별조치(SOLAS 11-2장)는 다음의 국제 항해에 종사하는 각 선박에 대하여 적용한다.

(1) 고속 여객선을 포함한 여객선

(2) 고속 화물선을 포함한 총톤수 500톤 이상의 화물선

(3) 이동식 해양구조물

(4) 국제항해에 종사하는 선박과 관련된 항만시설

3) 보안과 관련한 당사국 정부의 의무사항(제3규칙)

주관청 및 당사국 정부의 의무에 관한 사항으로 총 2개항으로 구성되어 있다.

제1항은 보안등급을 설정하고 기국선박에게 보안등급 정보의 제공 및 보안등급의 변동이 발생했을 때 최신화된 정보를 제공해야하는 주관청의 의무를 규정하고 있다.

제2항에서는 당사국 정부가 보안등급을 설정하여 자국 영토내의 항만시설과 항만에 입항하기 전 또는 항만에 정박해 있는 동안에 선박에게 보안등급 정보를 제공하도록 규정하고 있다.

4) 선박 및 회사의 요건(제4규칙)

총 5개항으로 구성되어 있으며 회사와 선박이 준수해야 할 규정, 선박과 항만의 보안등급이 상이할 경우 및 관련규정을 미준수할 때 취해야 할 조치 등에 관하여 규정하고 있다.

제1항에서는 회사로 하여금 ISPS Code B편의 지침을 고려하여 해상보안 특별조치(SOLAS 11-2장)와 ISPS Code A편의 규정을 준수하도록 하고 있다. 제2항에서는 회사와 같이 선박도 관련 규정을 준수하되 추가로 ISPS Code A편에 따라 그 준수여부를 심사받고 증서를 소지하도록 요구하고 있다. 제3항에서는 선박과 항만의 보안등급이 다를 경우 항만의 보안수준을 따르도록 하고 있다. 제4항 및 제5항에서는 선박은 부당하게 지체하지 말고 상위의 보안등급에 대응하여야 할 것과 관련 규정 미준수시에는 항만 입항 전 또는 선박/항만 인터페이스 중 먼저 발생하는 시기에 적절한 책임당국에 통보하여야 할 것을 요구하고 있다.

5) 회사의 구체적 책임사항(제5규칙)

이 규칙은 단일조항으로 구성되었으며 선박 운항에 대한 투명성을 나타내어 선박이 테러수단으로 이용되는 것을 방지하기 위한 사항을 규정하고 있다. 권한을 위임 받은 당사국 정부의 인원이 확인하고자 할 때 제공할 수 있도록 선장이 선원의 배승책임자 및 선박의 운항결정자 등과 관련된 정보를 본선에서 알 수 있도록 회사가 보장해 줄 의무를 부과하고 있다.

6) 선박보안경보시스템(제6규칙)

선박이 보안 위협을 당할 경우 기국 정부에 보고하여 가까운 연안국 등에 도움을 요청하기 위해 선박보안경보시스템이 도입되었다. 동 규칙은 총 7개항으로 구성되어 있으며 선종별 설치시기, 동 시스템의 요건, 경보시스템 수신시 주관청 및 체약당사국의 조치 등에 관해 규정하고 있다.

(1) 제1항에서는 선종별 설치시기를 아래와 같이 규정하고 있다.

① 2004. 7. 1 이후에 건조되는 모든 선박

② 2004. 7. 1 전에 건조된 고속여객선을 포함한 여객선은 2004. 7. 1. 후에 도래하는 첫 번째 무선설비검사 이전까지

③ 2004. 7. 1 전에 건조된 총톤수 500톤 이상의 유조선, 케미컬 탱커, 가스운반선, 벌크캐리어 및 고속화물선은 2004. 7. 1 후에 도래하는 첫 번째 무선설비검사 이전까지

④ 2004. 7. 1 전에 건조된 총톤수 500톤 이상의 기타 화물선 및 이동

식 해양구조물은 2006. 7. 1 후에 도래하는 첫 번째 무선설비검사 이전까지

(2) 제2항은 작동시 동 시스템의 요건을 아래와 같이 규정하고 있다.

① 주관청이 지정한 책임당국에 선박 대 육상 보안경보를 송신하여야 한다. 이 경우에 그 경보는 그 선박의 보안이 위협받거나 저해된다는 것을 알리면서 회사, 선박식별번호, 선박의 위치 등을 포함할 수도 있다.

② 타 선박에 선박보안경보를 송신하지 않아야 한다.

③ 선상에 어떤 알람도 울리지 않아야 한다.

④ 사유가 소멸되거나 재설정(reset)될 때까지 선박보안경보가 계속 발신되어야 한다.

(3) 제3항 및 4항에서는 동 시스템은 선교 및 최소한 다른 한 지역에서 추가로 작동되어야 하며 IMO에서 채택된 성능요건 이상의 요건 준수 및 부주의한 오작동 방지를 위해 동 시스템의 작동위치에 대한 설계 요건 등을 규정하고 있다.

(4) 제5항에서는 이 규칙의 요건을 만족한다면 제4장의 요건에 맞게 설치된 무선설비가 동 시스템을 대체할 수 있는 가능성을 열어 놓았다.

(5) 제6항 및 7항에서는 선박보안경보를 수신한 주관청 및 체약당사국은 그 선박이 운항 중에 있는 인근 연안국들에게 즉시 통보하도록 하고 있다.

7) 선박에 대한 위협(제7규칙)

입항선박의 보안을 위해 당사국 정부의 의무를 명확히 하기 위해 규정되었다. 당사국 정부는 보안등급을 설정하고 자국의 영해에서 운항하는 선박 또는 자국의 영해로 들어오려고 하는 선박에 대하여 보안등급에 관한 정보 및 관련 보안당국의 연락처 제공 등을 하여야 한다는 당사국 정부의 의무를 부과하고 있다(제1항 및 2항).

또한 공격위험이 있는 경우 당사국 정부는 당해 선박 및 기국 주관청에 현재의 보안등급, 선박에 의해 취해져야 하는 보안조치 및 선박의 보호를 위해 취하기로 결정한 보안조치 등에 관해 통보해야 한다(제3항).

8) 선박의 안전 및 보안에 대한 선장의 재량권(제8규칙)[9)]

9) 이 조항은 선장이 안전이나 보안 문제와 관련하여 결정하는 사항에 대하여 회사, 용선주 또는 기타 인원으로부터 간섭을 받지 않도록 보장할 것을 명확히 규정한 조항이다. 선장의 결정은 최우선적으로 보호되어야 하며 그 누구로부터 간섭 받지 않고 이루어져야 한

선박의 안전 및 보안을 확보하기 위하여 내리는 선장의 전문적 판단이 외부로부터 간섭받지 않도록 보호하기 위한 것으로 총 2개항으로 구성되어 있다.

선사, 용선주 등은 선장이 선박의 안전 및 보안을 유지하기 위해 자신의 전문적 판단에 의해 필요한 결정을 할 수 있도록 영향을 끼치지 않아야 한다(제1항).

선장의 전문적인 판단에 의하여, 선박운항 중 안전과 보안이 상충될 경우 선장은 선박의 안전을 유지하기 위하여 필요한 조치를 취하여야 한다. 그 경우 선장은 임시보안 조치를 취할 수 있으며 그 즉시 기국의 주관청에 통보하고, 필요한 경우 운항하고 있거나 입항하려는 항만의 당사국 정부에도 통보하여야 한다(제2항).

9) 통제 및 적합 조치(제9규칙)

항만국 통제를 통해 선박이 ISPS Code를 이행하도록 촉진하기 위한 사항을 규정하고 있다. 항만에 있는 선박에 대한 통제, 다른 당사국 정부의 항만에 입항하려는 선박 및 추가 규정 등 3부문으로 구분하여 규정하고 있으며 총 13개항으로 구성되어 있다.

(1) 항만내의 선박통제

SOLAS 11-2장의 적용을 받는 모든 선박은 다른 당사국 정부의 항만에서는 항만국 통제관에 의한 점검을 받아야 한다. SOLAS 11-2장 및 ISPS Code의 A편의 규정을 위반하였다는 명백한 근거가 없는 한 항만국통제는 선내에 비치된 국제선박보안증서 또는 임시국제선박보안증서의 유효성을 확인하는 점검으로 한정되어야 한다(1.1항).

관련규정을 위반하였다는 명백한 근거가 있거나 유효한 증서가 없는 경우에 항만국통제관은 적절한 규제조치를 부과하여야 한다. 이러한 규제는 ISPS Code의 B편을 고려하여 합당하게 부과되어야 한다(1.2항).

규제조치는 다음과 같은 것들이 될 수 있다(1.3항).

① 선박의 점검

다는 것을 명시하는 것이다. 본선에 있어서 안전과 보안에 관한 최고책임자가 선장이라는 사실 즉 선장의 권한을 한 번 더 확인시켜주는 것이며 또한 그 만큼 선장의 책임도 무거워졌다는 것을 말해주고 있다. 그리고 어떤 결정을 내릴 때 안전과 보안이 서로 상충될 경우에는 안전을 더 우선적으로 고려하라는 기준을 제시하고 있다. 그만큼 선박 및 승무원의 안전이 더 중요하다는 측면을 밝히고 있다. 그러나 이러한 경우에도 보안에 관한 조치는 완전히 무시하는 것이 아니고 할 수 있는 적절한 수준의 조치는 이행하여야 한다.

② 선박의 출항지연 및 선박의 억류,
③ 항만 내에서 이동을 포함한 운항의 제한
④ 항만으로부터 선박의 추방
⑤ 위에 추가하거나 양자택일하여 기타 더 약한 행정 또는 시정 조치를 포함할 수 있음

(2) 다른 당사국 정부의 항만에 입항하려는 선박

당사국 정부는 해상보안을 위해 자국항만에 입항하는 선박에 대해 항만국통제관에게 아래 정보를 제공하도록 요구할 수도 있다(2.1항). 이는 입항 전 선박이 관련 규정을 준수하도록 하여 선박 억류 등 여러 가지 규제를 사전에 예방하기 위한 것이다. 그러나 선장은 그런 정보의 제공을 거부할 수 있으며 이 경우 선장은 입항이 거부될 수도 있다는 것을 전제로 해야 한다(2.2항).

① 유효한 증서 소지 여부 및 발행당국의 이름
② 현재 선박의 보안등급
③ 선박/항만 인터페이스를 수행했던 이전 항만에서 선박이 운용한 보안등급(최근 10회 범위 내)
④ 이전 항만에서 취한 특별한 또는 추가된 보안조치(최근 10회 범위 내)
⑤ 선박 대 선박 활동에서 유지된 적절한 선박보안 절차(최근 10회 범위 내)
⑥ ISPS Part B의 지침을 고려한 기타 실질적인 보안 관련 정보(선박보안계획서의 세부사항은 아님)

만약 당사국 정부의 요청이 있다면 위 정보에 대해 회사 또는 선박은 당사국 정부가 수용할 수 있을 정도의 증거자료를 제공해야 한다(2.1항). 또한 입항하려는 선박의 경우 지난 항만시설 방문관련 최소 10회 이상의 기록을 유지하여야 한다(2.3항).

항만국통제관이 위 정보를 수령한 후에 입항하려는 선박이 관련 규정을 위반하였다는 명백한 근거가 있는 경우에는 위반사항을 시정하기 위하여 선박 및 주관청과 연락을 시도하여야 한다. 이 경우에도 시정되지 않거나 또는 항만국통제관이 그 선박이 관련 규정을 위반하고 있다는 다른 명백한 근거가 있는 경우에는 규정한 아래의 조치를 취할 수 있다(2.4항).

항만국통제관이 취할 수 있는 조치는 다음과 같다(2.5항).

① 위반사항의 시정

② 그 당사국 정부의 내수면 또는 영해의 특정지역으로 이동
③ 선박의 점검(당사국 정부의 영해에 있는 경우)
④ 입항 거부

그런 조치를 취하기 전에 당사국 정부는 그 선박에 의도를 명확히 통보하여야 하며, 그 통보에 근거해 선장은 입항을 철회할 수 있다. 이 경우 이 규칙은 적용되지 않는다.

(3) 추가 규정(Additional provisions)

총 5개항으로 구성되어 있으며 당사국 정부가 위반선박에 대한 규제 후 주관청 등에 대한 신속한 정보제공, 입항거부 및 강제출항 등의 빈발을 방지하기 위한 규정 등에 관해서 언급하고 있다.

제3.1항에서는 아래 2가지의 경우에 대해 항만국통제관이 부과한 규제, 취한 조치, 그 사유 등에 관해서 서면으로 주관청에 통보하도록 하고 있다. 또한 위 규제 시에 그 당사국 정부는 관련된 선박에 관한 증서를 발행한 보안인증심사대행기관 및 국제해사기구에도 통보해야 한다.

① 1.3항에서 언급된 규제보다 더 약한 행정 또는 시정조치 외에 규제를 부과한 경우
② 2.5항에서 언급된 조치가 취해진 경우

제3.2항에서는 입항이 거부되거나 추방된 경우에 항만당국이 차기 기항지의 항만당국 및 기타 관련 연안국에 필요한 사실을 통보하도록 하고 있다. 이 경우에 그런 통보에 대한 비밀과 보안이 유지되어야 한다.

제3.3항에서는 2.4항 및 2.5항에 따른 입항 거부 또는 1.1항에서 1.3항에 따른 항만추방은 명백한 근거를 가지는 경우에만 이루어지도록 하고 있다. 즉, 그 위협을 제거할 다른 적절한 수단이 없거나 그 선박이 다른 재산, 선박 또는 인명의 안전 및 보안에 직접적인 위협을 준다고 믿는 명백한 근거가 있어야 한다. 이런 근거의 판단은 전적으로 항만국통제관의 몫이다.

제3.4항에서는 1.3항의 규제와 2.5항의 조치들은 이 규칙에 따라 한시적으로 부과되도록 하고 있다. 이 기한은 당사국 정부가 만족할 정도로 위반사항이 시정되었다고 판단할 때까지이다.

제3.5항에서는 당사국 정부가 항만에서 규제하거나 또는 입항하려는 선박의 위반사항에 대해 조치할 경우에는 아래원칙에 따르도록 하고 있다.

① 대상선박의 과도한 억류나 지체가 없도록 가능한 모든 노력이 기울여 져야 하고, 만약 부당한 억류가 발생된 경우에는 손실을 겪거나 및 피해를 당한 선박에게 보상을 받을 권리를 부여하여야 한다.

② 비상시 또는 인명을 구하기 위한 인도주의적 사유 또는 보안을 목적으로 하는 경우에는 선박에 필요한 접근이 이루어지도록 한다.

10) 항만시설에 대한 요건(제10규칙)

총 3항으로 구성되어 있으며 보안을 위해 항만시설이 준수해야 할 규정, 항만시설의 보안평가 및 보안계획서에 대한 당사국 정부의 의무 등에 관해 규정하고 있다.

제1항에서는 ISPS Code B편의 지침을 고려하여 해상보안특별조치(SOLAS 11-2장)와 ISPS Code A편의 규정에 대한 항만시설의 준수요건을 규정하고 있다.

제2항에서는 자국의 영토 내에 항만시설을 가진 당사국 정부는 ISPS Code A편의 규정에 따라 항만보안평가를 수행·검토하고 승인하도록 하고 있다. 또한 항만보안계획서도 ISPS Code A편의 규정에 따라 개발, 검토, 승인 및 이행되도록 규정하고 있다.

제3항에서는 당사국 정부는 보안선언서의 제출이 요구될 때를 포함하여 다양한 보안등급에 따라 항만보안계획서에 포함되도록 요구되는 조치를 지정해서 알리도록 하고 있다.

11) 대체보안협정(제11규칙)

총 4개항으로 구성되어 있으며 고정된 단거리 국제항해에 한해 해상보안규정을 대체할 수 있는 양자 및 다자협정을 체결할 수 있도록 하고 있다.

제1항에서는 한 체약당사국은 각국의 영해 내에 있는 항만시설간 고정항로에 관한 단거리 국제항해를 포함하는 대체 보안규정에 대하여 다른 체약당사국과 서면으로 양자 또는 다자간 협정을 체결할 수 있도록 하고 있다.

제2항에서는 그런 경우에 그 협정의 적용대상이 아닌 항만시설 및 다른 선박의 보안수준을 저해하지 않도록 하고 있다.

제3항에서는 협정의 적용대상선박은 협정에 포함되지 않는 선박과 선박대 선박의 활동을 수행하지 못하도록 하고 있다.

제4항에서는 축적된 경험과 어떤 상황 또는 선박 및 항만의 보안에서 평

가된 위협의 변화를 고려하여 그런 협정을 주기적으로 검토하도록 하고 있다.

12) 동등한 보안규정(제12규칙)

총 2항으로 구성되어 있으며 주관청이 자국적 선박과 자국의 항만시설에 대해 SOLAS 11-2장과 ISPS코드 A편에서 규정한 것과 최소한 동일한 효과가 있는 다른 보안조치를 이행할 수 있도록 하고 있다. 이 경우에 주관청은 이러한 내용에 관해 IMO에 통보하여야 한다.

13) 정보의 전달(제13규칙)[10)]

총 7개항으로 구성되어 있으며 당사국 정부가 IMO 에 통보해야하는 내용에 대해 언급하고 있다.

제1항에서는 당사국 정부가 2004. 7. 1 이전까지 다음사항을 IMO에 통보하여 회사 및 선박에서 그 정보를 이용할 수 있도록 하고 있다. 또한 당사국 정부는 변경될 때 최신화 해야 하며 IMO는 타 당사국 정부가 그런 정보를 회람시키도록 규정하고 있다.

(1) 선박 및 항만시설에 책임이 있는 국내 주관청의 명칭 및 상세한 연락처
(2) 승인된 항만시설보안계획서에 포함된 당사국 정부의 영해 내의 위치들
(3) 선박 대 육상 보안경보를 항상 수신하고 조치하도록 지정된 전담자들의 성명 및 상세한 연락처
(4) 통제 및 그 이행조치를 하면서 당사국 정부로부터 항상 정보를 받고 조치하도록 지정된 전담자들의 성명 및 상세한 연락처
(5) 선박에 대한 지원 및 자문을 제공하기 위해 지정된 24시간 전담자들의 성명 및 상세한 연락처

제2항에서는 당사국 정부는 2004. 7. 1 이전까지 그런 인증기관에 위임된 권한의 조건 및 책임의 상세와 더불어 보안인증심사대행기관의 명칭과 상세한 연락처를 IMO에 통보하도록 하고 있다.

제3항에서는 당사국 정부는 2004. 7. 1 이전까지 IMO에 승인된 항만시설

10) 국제해사기구는 각 당사국 정부가 SOLAS 제11-2장 제13규칙에 따라 보고하는데 사용하도록 인터넷 시스템을 개발하였다. 전 세계 통합해운정보시스템(Global Integrated Shipping Information System, GISIS)으로 명칭이 부여되었으며 IMO Home Page로 접속하여 이용할 수 있다. 이 시스템은 정보의 입력뿐만 아니라 다른 당사국 정부가 입력한 정보를 조회할 수도 있도록 되어 있다.

보안계획서의 목록을 제출하여야 하며, 동 계획서에 포함된 위치를 계획서의 승인일과 함께 제시하도록 하고 있다. 뿐만 아니라 이후에 일어날 변화에 대해서도 통보해야 한다.

제4항에서는 당사국 정부는 2004. 7. 1. 이후에 5년의 주기로 승인된 항만시설보안계획서를 개정하고 최신화하여 그 목록을 IMO에 제출하도록 하고 있다. 또한 동 계획서에 포함된 위치 및 동 계획서의 승인일(및 그 개정된 계획서의 승인일)을 함께 제시하도록 하고 있다.

제5항에서는 당사국 정부는 제11규칙 하에서 체결된 협정에 관한 아래의 정보를 IMO에 제공하도록 하고 있다.

(1) 협정을 체결한 당사국 정부의 명칭

(2) 협정에 포함된 고정항로와 항만시설

(3) 협정검토의 주기

(4) 협정의 발효일

(5) 타 당사국 정부와의 협의 시에 발생한 정보

그 후에 가능한 한 곧 협정이 개정되거나 종료될 때 관련 정보를 IMO에 제공해야 한다.

제6항에서는 제12규칙 하에서 자국적 선박 및 자국의 영토 내에 있는 항만시설에 대해 동등한 안전규정을 사용토록 한 당사국 정부는 그 사실을 IMO에 통보하도록 하고 있다.

제7항에서는 국제해사기구는 다른 당사국 정부가 요구할 경우에 제3항의 규정에 따라 전달된 정보를 제공하도록 규정하고 있다.

제5절 ISPS Code 구성 및 내용

1. ISPS Code의 종류 및 성격

ISPS Code는 A편과 B편으로 나누어져 있다(<표 2-2> 참조). A편에는 선박이나 항만시설이 보안시스템을 수립하고 유지하는데 강제적으로 적용되어야 하는 요구사항이 규정되어 있는 규칙이며, B편에는 SOLAS 제11-2장 및 ISPS Code A편에 규정된 요구사항을 실행할 때 고려하여야 하는 지침이 규정되어 있다.

<표 2-2> ISPS Code의 종류

구 분	제 목
ISPS Code A편	개정된 1974 SOLAS 협약 제11-2장의 규정과 관련된 강제요건 (Mandatory Requirements Regarding the Provisions of Chapter XI-2 of the International Convention for the Safety Of Life At Sea, 1974, as amended)
ISPS Code B편	1974 해상인명안전협약의 부속서 제11-2장 및 국제 선박 및 항만시설 보안규칙 A편의 규정에 관한 지침서 (Guidance Regarding the Provisions of Chapter XI-2 of the annex to the International Convention for the Safety Of Life At Sea, 1974 as amended and Part A of this code)

선박이나 항만시설이 SOLAS 제11-2장에 따른 보안시스템을 수립하기 위해서는 강제적으로 적용되는 SOLAS 11-2장 및 ISPS Code A편에 규정된 요건들을 따라야 한다. 그러나 SOLAS 11-2장 및 ISPS Code A편에는 보안시스템에 포함되어야 하는 기본적인 원칙에 해당되는 사항들만 규정하고 있다. 그래서 항만시설이 보안시스템을 구성할 때는 이 기본적인 원칙들을 수용하여 시행하기 위한 구체적인 방법을 모색하여야 한다. 이 구체적인 방법에 대한 지침을 제공하는 것이 ISPS Code B편이다. 그러므로 B편은 비록 강제적으로 적용되는 규정은 아니라고 하지만 보안시스템을 수립할 때는 반드시 참조하여야 하는 규정이므로 실질적인 의미에서는 SOLAS 11-2장이나 ISPS Code A편과 동일하게 강제적으로 적용되는 규정이라고 보아야 한다. 항만시설의 경우에는 선박에 적용되는 항만국 통제 같은 제도가 없으므로 ISPS Code B편을 강제적으로 적용하느냐 하지 않느냐는 당사국 정부가 결정하여 시행하면 된다. 그러나 선박의 경우에는 항만국 통제를 시행할 때 이러한 부분에 대해서 논란이 야기될 수 있으므로 이런 논란이 발생할 것을 미리 예상하여 국제해사기구에서는 ISPS Code B편의 해당 부분을 강제 규정으로 해석한다고 추가로 규정하였다.[11)]

2. ISPS Code의 구성

선박 또는 항만시설이 보안시스템을 수립 및 유지하기 위해서는 ISPS Code

11) IMO MSC/Circ.1097 : 2003년 6월 개최한 제77차 MSC회의에서 채택되었다.

A편 및 B편을 같이 준수하여야 한다고 앞에서 언급하였다. 그래서 사용자들이 쉽게 활용할 수 있도록 ISPS Code A편과 B편은 동일한 순서의 번호 체계를 취하고 있다. 즉 A편에 규정된 사항에 대한 지침을 보고자하면 동일한 번호의 B편의 내용을 참조하면 된다(<표 2-3> 참조).

<표 2-3> ISPS Code A편, B편 구성

번 호	제 목
1	일반사항(General)
2	정의(Definitions)
3	적용(Application)
4	당사국 정부의 책임(Responsibilities of Contracting Governments)
5	보안선언서(Declaration of security)
6	회사의 의무(Obligations of the Company)
7	선박보안(Ship security)
8	선박보안평가(Ship security assessment)
9	선박보안계획서(Ship security plan)
10	기록(Records)
11	회사보안책임자(Company security officer)
12	선박보안책임자(Ship security officer)
13	선박보안의 교육, 훈련 및 연습(Training, drills and exercises on ship security)
14	항만시설보안(Port facility security)
15	항만시설보안평가(Port facility security assessment)
16	항만시설보안계획서(Port facility security plan)
17	항만시설보안책임자(Port facility security officer)
18	항만시설보안에 관한 교육, 훈련 및 연습(Training, drills and exercises on port facility security)
19	선박의 심사 및 증서발급(Verification and certification for ships)

3. ISPS Code A편의 내용

1) 일반사항(제1절)

개요, 목적 및 기능적 요건을 규정하고 있다.

(1) 개요

A편은 SOLAS 11-2장에서 언급된 강제규정을 다루고 있음을 밝히고

있다.

(2) 목적

ISPS Code의 목적을 다음과 같이 규정하고 있다.

① 보안위협을 탐지하기 위한 국제적 체계를 수립하고 국제무역에 사용되는 선박 또는 항만시설에 영향을 미치는 보안사건에 대한 예방조치를 취하기 위함.

② 해상보안을 보장하기 위하여 당사국 정부, 정부기관, 지방관청과 해운 및 항만업자의 역할과 임무를 국내적으로 그리고 국제적으로 수립함.

③ 보안관련 정보를 조기에 효과적으로 수집하고 교환하는 것을 보장하기 위함.

④ 적절하고 알맞은 해상보안대책이 적소에 취해지고 있다는 확신을 주기 위함.

(3) 기능적 요건[12)]

ISPS Code의 목적을 달성하기 위하여 다음과 같은 기능적 요건들을 필요로 하고 있음을 규정하고 있다.

① 보안위협과 관련된 정보의 수집과 평가, 그리고 관련 당사국 정부와의 정보 교환

② 선박과 항만시설을 위한 통신규약 유지

③ 선박, 항만시설 및 제한구역에 대한 비인가 접근방지

④ 선박 또는 항만시설에 비인가 무기, 방화 장비 또는 폭발물의 반입방지

⑤ 보안위협 또는 보안사건에 대응하여 경보 발생 수단 제공

⑥ 보안평가에 근거한 선박 및 항만시설보안계획서 필요

⑦ 보안계획과 절차에 익숙해지도록 교육, 훈련 및 연습 필요

2) 정의(제2절)

ISPS Code에 사용되는 용어에 대한 정의를 규정하고 있으며, 다음과 같은 사항들이 포함되어 있다.

(1) 선박보안계획서

(2) 항만시설보안계획서

(3) 선박보안책임자

---

12) 기능적 요건이란 ISPS Code의 목적을 달성하기 위하여 필요한 주요 기능을 나타내고 있는 것이다. 기능적 요건은 보안시스템을 구성하는 주된 부분이 되며, 이에 대하여는 ISPS Code 제4절부터 구체적으로 전개되어 진다.

(4) 회사보안책임자

(5) 항만시설보안책임자

(6) 보안등급 1, 2. 3[13)]

3) 적용(제3절)

ISPS Code가 적용되는 대상에 대하여 규정하고 있다. SOLAS 11-2장에서 규정된 적용범위와 서로 다르지 않다. 다만, 국제항해에 종사하지 않는 선박이 주로 이용하는 항만시설을 간헐적으로 국제항해에 종사하는 선박이 이용하는 경우에 ISPS Code를 어떤 범위까지 적용할 것인지 당사국 정부가 결정하도록 요구하고 있으며, 이 경우 반드시 ISPS Code A편에 따라 항만시설보안평가를 근거로 결정을 내려야 한다고 규정하고 있다.[14)]

4) 당사국 정부의 책임(제4절)

총 4개항으로 구성되어 있으며 당사국 정부가 보안등급을 설정할 때 고려하여야 하는 요소, 보안인증심사대행기관에 대행시킬 수 없는 사항 및 승인된 선박보안계획서 또는 항만시설보안계획서에 대한 효과성을 확인할 것을 규정하고 있다.

(1) 당사국 정부는 보안등급을 설정하여야 하고 보안사건을 예방하기 위한 지침을 제공하여야 한다. 보안등급을 설정할 대 고려되어야 하는 요소는 다음과 같다.

① 위협정보의 신뢰성 정도

② 위협정보의 확증 정도

③ 위협정보의 구체성 또는 긴급성 정도

---

13) 보안등급 1, 2, 3은 다음과 같이 구분된다.
보안등급 1 : 최소한의 적절한 방어적 보안조치가 항상 유지되어야 하는 수준, 선박과 항만시설이 일상적으로 운영되는 수준으로 평상수준을 말함.
보안등급 2 : 일정기간동안 적절한 추가의 방어적 보안조치가 유지되어야 하는 수준, 보안사건에 대한 증대된 위험이 있는 동안 적용되는 수준으로 경계수준을 말함.
보안등급 3 : 제한된 기간동안 보다 구체적인 방어적 보안조치가 유지되어야 하는 수준, 보안사건의 가능성이 있거나 급박한 위험이 있는 기간동안 적용되는 수준으로 비상수준을 말함.

14) 국제항해에 종사하는 선박이 전적으로 이용하는 항만시설이 아닌 경우에도 보안시스템 적용에는 예외가 될 수 없음을 나타내고 있으며, 어느 정도의 범위까지 적용할 것인지는 당사국 정부가 결정하도록 하고 있다. 단, 이 결정은 SOLAS 제11-2장이나 ISPS Code A편에서 요구하는 수준을 손상시켜서는 안 된다고 규정하고 있다. 보안에 관하여는 취약성이 발생할 수 있는 예외 사항을 허용할 수 없음을 나타내고 있는 조항이라고 볼 수 있다.

④ 보안사건이 가져올 수 있는 잠재적 결과

(2) 보안등급 3을 설정한 경우에는 필요하다면 적절한 보안지침을 발행하여야 하며 영향을 받을 수 있는 선박 및 항만시설에 관련 정보를 제공하여야 한다.

(3) 당사국 정부는 SOLAS 11-2장 및 ISPS Code A편에 규정된 당사국 정부의 의무 사항 중 일부를 보안인증심사대행기관에 위임할 수 있으나 다음 사항은 예외로 한다.

① 보안등급 설정

② 항만시설보안평가의 승인

③ 항만시설보안책임자 지정이 필요한 항만시설 결정

④ 항만시설보안계획서의 승인

⑤ 항만국 통제

⑥ 보안선언서 요건 수립

(4) 당사국 정부는 승인한 선박보안계획서 또는 항만시설보안계획서에 대한 효과성을 확인하여야 한다.[15)]

5) 보안선언서(제5절)

총 7개항을 구성되어 있으며 당사국 정부가 보안선언서에 대하여 결정하여야 하는 사항, 선박에서 보안선언서를 제출할 수 있는 조건 및 기타 보안선언서 작성 및 유지에 필요한 사항을 언급하고 있다.

(1) 당사국 정부는 언제 보안선언서를 작성하여야 하는지 결정하여야 한다.

(2) 다음과 같은 경우 선박은 보안선언서 작성을 요청할 수 있다.

① 인터페이스를 하고 있는 항만시설 또는 다른 선박보다 상위의 보안등급으로 선박이 운항하고 있는 경우

② 국제항로 또는 이들 항로를 운항하고 있는 특정선박에게 적용하는 보안선언서에 관한 당사국 정부간 협정이 있는 경우

③ 적용 가능한 선박 또는 항만시설에 영향을 미치는 보안위협 또는 보안사건이 있었던 경우

④ 승인된 항만시설보안계획서의 소지 및 시행이 요구되지 아니하는 항만에 선박이 있는 경우

⑤ 승인된 선박보안계획서의 소지 및 시행이 요구되지 아니하는 다른

15) 효과성을 확인하는 것은 초기 인증 및 인증 유지를 위한 심사를 시행하는 것을 의미한다.

선박과 선박 대 선박 활동을 수행하는 경우

(3) 항만시설 또는 선박은 보안선언서 작성이 요청되면 이를 완성하여야 한다.

(4) 보안선언서는 다음 인원에 의하여 완성되어야 한다.

① 선장 또는 선박보안책임자

② 항만시설보안책임자 또는 당사국 정부가 달리 결정한 경우 항만시설을 대표하여 육상 보안 담당 기관

(5) 보안선언서는 선박과 항만시설 간 또는 선박 간에 공유될 수 있는 보안요건을 표시하여야 한다.

(6) 당사국 정부는 항만시설이 보안선언서를 보유하여야 하는 최소 기간을 명시하여야 한다.

(7) 주관청은 기국선박이 보안선언서를 보유하여야 하는 최소 기간을 명시하여야 한다.

6) 회사의 의무(제6절)

총 2개 항으로 구성되어 있으며 회사가 선장에게 안전 및 보안에 관한 최우선적인 권한을 부여하고 있음을 명확히 나타내도록 규정하고 있다.

(1) 회사는 선박보안계획서에 선장이 선박의 안전 및 보안과 관련된 결정을 하고 필요한 경우 당사국 정부 또는 회사에게 지원을 요청할 수 있는 최우선적인 책임 및 권한을 가지고 있음을 명시하여야 한다.[16)]

(2) 회사는 회사 보안책임자, 선장 및 선박보안책임자가 SOLAS 11-2장 및 ISPS Code A편에 따라 의무와 책임을 수행할 수 있도록 필요한 지원의 제공을 보장하여야 한다.

7) 선박보안(제7절)

총 9개 항으로 구성되어 있으며 선박에서 보안활동을 수행하여야 하는 구체적인 대상을 규정하고 있으며 보안등급의 변경에 대한 대응 절차를 언급하고 있다.

(1) 보안등급 1에서 모든 선박은 ISPS Code B편의 지침을 반영하여 다음 활동이 수행되도록 하여야 한다.

① 선박의 모든 보안 임무 수행

② 선박에의 접근 통제

16) 이 조항은 SOLAS 제11-2장 8규칙에서 규정한 선장의 재량권을 구체적으로 적용하도록 규정하고 있는 조항이다. 즉 선장이 최우선적인 책임 및 권한을 가지고 있음을 명확하게 선박보안계획서에 규정할 것을 요구하고 있다.

③ 인원 및 인원들이 소지한 소지품의 승선 통제
④ 인가 받은 자만이 접근할 수 있는 제한구역 감시
⑤ 선박의 주변지역 및 갑판구역 감시
⑥ 화물 및 선용품 취급 감독
⑦ 보안통신 이용 보장

(2) 보안등급 2 및 3에서는 보안등급 1에서 수행하는 보안활동에 부가하여 추가적인 방어조치(보안등급 2) 및 강화된 특정보호조치(보안등급 3)가 수행되어야 한다.

(3) 보안등급 2 또는 보안등급 3을 설정한 당사국 정부의 항구에 입항하기 전이거나 입항 중에 있는 선박은 보안등급이 변경되었다는 지침을 접수하였음을 통보하여야 하며 항만시설보안책임자에게 선박보안계획서에 따라 적절한 보안조치 및 절차의 시행이 개시되었음을 통보하여야 한다.

(4) 이미 입항해있거나 입항 예정인 항만의 보안등급보다 더 높은 보안등급을 설정하도록 주관청으로부터 선박이 통보 받으면 그 선박은 지체없이 항만시설의 당사국 정부 및 항만시설보안책임자에게 통보하여야 한다.

8) 선박보안평가(제8절)

총 5개 항으로 구성되어 있으며 선박보안평가에 포함되어야 하는 사항들에 대하여 규정하고 있다.

(1) 선박보안평가는 선박보안계획서를 개발하고 개정하는 과정의 필수적인 단계이며 전문가에 의하여 수행되도록 하여야 한다.

(2) 선박보안평가는 현장보안검사를 하여야 하고 또한 다음 요소들을 포함하여야 한다.

① 시행중인 보안조치, 절차 및 활동에 대한 식별
② 중요하게 보호되어야 하는 본선의 주요 작업의 식별 및 평가
③ 본선의 주요 작업에 대해 발생할 수 있는 위협 및 발생가능성의 식별 및 평가
④ 기반시설, 정책 및 절차에 있어서 인적요소를 포함한 취약점의 식별

(3) 선박보안평가는 회사에 의해 문서화, 검토, 수락 및 보유되어야 한다.

9) 선박보안계획서(제9절)

총 8개 항으로 구성되어 있으며 선박보안계획서에 포함되어야 하는 내용 및 선박보안계획서를 유지 관리하기 위한 사항들이 규정되어 있다.

(1) 선박은 주관청이 승인한 선박보안계획서를 본선에 비치하여야 한다. 선박보안계획서에는 3가지 보안등급에 대한 조치들이 규정되어 있어야 한다.

(2) 주관청은 선박보안계획서의 검토 및 승인 업무를 보안인증심사대행기관에 위임할 수 있다.

(3) 선박보안계획서 승인 또는 이미 승인된 선박보안계획서의 개정 승인을 받기 위해서는 선박보안계획서 개발에 근거가 된 선박보안평가를 같이 제출하여야 한다.

(4) 선박보안계획서는 ISPS Code B편에 있는 지침을 고려하여 개발되어야 하며 본선에서 사용되는 언어로 작성되어야 한다. 만약 그 언어가 영어, 불어 또는 스페인어가 아니라면 이 중 하나로 번역되어야 한다.[17] 선박보안계획서에는 최소한 다음 사항이 포함되어야 한다.

① 사람, 선박 또는 항만을 대상으로 사용될 의도가 있는 무기, 위험물질 및 장치와 승인되지 않은 운송을 방지하기 위해 계획된 수단

② 제한구역의 식별 및 동 구역에 비인가자의 접근을 방지하기 위한 조치

③ 선박에 대한 비인가 접근을 방지하기 위한 조치

④ 선박 또는 선박/항만 인터페이스의 중요 작업을 수행하기 위한 규정을 포함하여 보안위반 또는 보안위협에 대응하는 절차

⑤ 보안등급 3에서 당사국 정부가 내릴 수 있는 보안지시사항을 따르기 위한 절차

⑥ 보안위협 또는 보안위반의 경우 피난 절차

⑦ 보안측면에서 보안임무가 지정된 인원 및 기타 본선근무자의 임무

⑧ 보안활동의 심사를 위한 절차

⑨ 선박보안계획서에 연관된 교육, 훈련 및 연습을 위한 절차

⑩ 항만시설 보안활동과의 인터페이스를 위한 절차

⑪ 선박보안계획서의 정기적 검토 및 최신화를 위한 절차

⑫ 보안사건의 보고를 위한 절차

⑬ 선박보안책임자 식별

⑭ 24시간 연락 가능한 세부 사항을 포함하여 회사보안책임자 식별

17) 본선에서 사용하는 언어가 영어, 불어, 스페인어가 아닌 경우에는 선박보안계획서를 2권으로 작성하거나 이들 언어와 병기를 하여 구성하여야 한다.

⑮ 선박 보안장비의 검사, 테스트, 교정 및 유지를 보장하기 위한 절차

⑯ 본선에 비치된 보안장비의 테스트 또는 교정주기

⑰ 선박보안경보시스템 설치된 위치 식별

⑱ 오경보 발생을 막기 위하여 테스트, 작동, 해제 및 재설정을 포함한 선박보안경보시스템을 사용하기 위한 절차, 지침

(5) 내부심사를 수행하는 자는 심사대상이 되는 활동과는 무관하여야 한다.[18)]

(6) 주관청은 승인된 선박보안계획서 또는 승인된 보안계획서에 명시된 보안장비를 변경하는 경우 주관청에 의해 변경 사항이 승인될 때까지 그 변경사항이 시행되어서는 안 되는 사항들을 결정하여야 한다.

(7) 선박보안계획서는 비인가자의 접근 또는 폭로로부터 보호되어야 한다.

(8) 선박보안계획서는 항만국 통제관으로부터 검사를 받아야 하는 대상이 아니다. 단, 항만국 통제관이 판단할 대 본선이 SOLAS 11-2장 및 ISPS Code A편을 따르지 아니하며 이를 검증하기 위한 유일한 수단이 선박보안계획서의 관련 요건을 확인하는 것이라는 명백한 근거가 있을 때에만 부적합사항과 관련된 부분에 대하여 제한적으로 열람이 가능하다. 이 경우에도 ISPS Code A편 제9.4절의 ②, ④, ⑤, ⑦, ⑮, ⑰ 및 ⑱은 당사국 정부의 동의가 없는 한 검사 대상이 될 수 없다.[19)]

10) 기록(제10절)

총 4개 항으로 구성되어 있으며 본선에서 보안활동을 하고 유지하여야 하는 기록의 관리에 대하여 규정하고 있다.

(1) 다음 보안활동과 관련된 기록들에 대하여 최소한 주관청이 정한 기간 동안 본선에 보유하여야 한다.

① 교육, 훈련 및 연습

② 보안위협 및 보안사건

③ 보안위반

④ 보안등급의 변경

---

18) 내부심사의 객관성을 유지하기 위하여 본선에 승선하고 있는 인원이 자기 선박에 대한 내부심사를 수행할 수 없도록 규정한 조항이다.

19) 이 사항은 선박보안에 민감한 사항이므로 항만국 통제를 담당하는 책임자라고 해도 당사국 정부의 동의가 없으면 검사 대상이 될 수 없음을 강조하고 있다.

⑤ 선박에 대한 구체적인 위협 또는 현재 또는 이전에 기항했던 항만 시설에 대한 구체적인 위협과 같이 선박 보안과 직접적으로 연관된 통신
⑥ 보안활동에 대한 내부심사 및 검토
⑦ 선박보안평가의 정기적 검토
⑧ 선박보안계획서의 정기적 검토
⑨ 선박보안계획서의 개정 사항
⑩ 선박보안경보시스템의 테스트를 포함하여 본선에 설치된 보안장비의 유지, 교정 및 테스트

(2) 보안활동 기록은 본선의 사용 언어로 기록되어야 하며 사용 언어가 영어, 불어 또는 스페인어가 아닌 경우 이들 언어 중 하나로 번역되어야 한다.

(3) 보안활동 기록은 비인가 된 접근 또는 폭로로부터 보호되어야 한다.

11) 회사보안책임자(제11절)

총 2개 항으로 구성되어 있으며 회사보안책임자의 의무와 책임에 대하여 언급하고 있다.

(1) 회사는 회사보안책임자를 지정하여야 한다. 선종 또는 선박 척수에 따라 각 보안책임자가 어떤 선박에 책임을 맡고 있는지가 명확히 구분이 된다면 다수 인원을 회사보안책임자로 임명할 수 있다.

(2) 회사보안책임자는 최소한 다음의 책임과 의무를 가진다.
① 선박이 직면할 수 있는 위협수준을 통보
② 선박보안평가가 수행되도록 보장
③ 선박보안계획서 개발, 선박보안계획서 승인을 받기 위한 제출, 동 계획서의 실행 및 유지를 보장
④ 결함보완 및 각 선박의 보안요건을 만족시키기 위하여 선박보안계획서의 적절한 수정을 보장
⑤ 보안활동에 대한 내부심사 및 검토 준비
⑥ 선박의 최초 및 사후 심사를 주관청 또는 보안인증심사대행기관에 신청
⑦ 내부심사, 정기적인 검토, 보안 점검 및 적합성 검증 중에 식별된 결함 및 부적합사항이 즉시 처리되도록 보장
⑧ 보안의식 및 경계를 강화
⑨ 선박의 보안책임을 맡고 있는 담당자에 대한 적절한 교육 보장

⑩ 선박보안책임자와 관련 항만시설보안책임자간의 효과적 의사소통과 상호조정을 보장
⑪ 보안요건과 안전요건 사이의 일관성 보장
⑫ 동형선 또는 선단 보안계획서가 기본적으로 사용된다면 각 선박에 대한 계획서에 선박의 특정 정보가 정확하게 반영되도록 보장
⑬ 특정 선박 또는 다수 선박에 대하여 승인된 대안 또는 동등한 계획의 실행 및 유지를 보장

12) 선박보안책임자(제12절)

총 2개 항으로 구성되어 있으며 선박보안책임자의 의무와 책임에 대하여 규정하고 있다.

(1) 선박보안책임자는 각 선박에 임명되어야 한다.

(2) 선박보안책임자는 최소한 다음의 책임과 의무를 가진다.

① 적절한 보안조치의 유지를 보장하기 위해 주기적인 선박보안점검 수행
② 수정된 사항을 포함하여 선박보안계획서의 실행을 유지하고 감독
③ 화물 및 선용품 취급에 대한 보안 측면을 선내의 다른 인원 및 관련 항만시설 보안책임자와 상호 조정
④ 선박보안계획서의 수정을 제안
⑤ 내부심사, 정기적인 검토, 보안점검 및 적합성검증 동안에 식별된 결함, 부적합사항 및 시정조치의 실행을 회사보안책임자에게 보고
⑥ 보안의식 및 선상경계를 강화
⑦ 선내근무자에 대한 적절한 교육이 제공되도록 보장
⑧ 모든 보안사건을 보고
⑨ 선박보안계획서를 실행하는데 있어서 회사보안책임자 및 관련 항만시설보안책임자 상호 협조
⑩ 보안장비가 있는 경우 이들 장비의 적절한 운용, 시험, 교정 및 유지 관리를 보장

13) 선박보안의 교육, 훈련 및 연습(제13절)

총 5개 항으로 구성되어 있으며 회사보안책임자, 육상근무자, 선박보안책임자 및 본선 근무자들에 대한 교육, 연습 및 훈련에 대하여 언급하고 있다.

(1) 회사보안책임자와 관련 있는 육상근무자는 ISPS Code B편에 있는

지침을 고려하여 지식을 보유하여야 하고 훈련을 받아야 한다.

(2) 선박보안책임자는 ISPS Code B편에 있는 지침을 고려하여 지식을 보유하여야 하고 훈련을 받아야 한다.

(3) 보안에 대한 특정한 임무 및 책임이 있는 선상근무자는 선박보안계획서에 규정된 선박보안에 대한 자신의 임무를 이해하고 있어야 하며 ISPS Code B편에 있는 지침을 고려하여 부여된 임무수행을 위한 충분한 지식 및 능력을 갖추어야 한다.

(4) 선박보안계획서가 효과적으로 시행되도록 하기 위하여 ISPS Code B편에 있는 지침을 고려하여 적절한 간격을 훈련이 실시되어야 한다.

(5) 회사보안책임자는 적절한 간격으로 연습에 참여하여 선박보안계획서가 효과적으로 시행되도록 보장하여야 한다.

14) 항만시설보안(제14절)

총 6개 항으로 구성되어 있으며 항만시설이 보안활동을 수행하여야 하는 구체적인 대상을 규정하고 있으며 보안등급의 변경에 대한 대응 절차와 선박과의 상호교신에 대하여 규정하고 있다.

(1) 항만시설은 당사국 정부가 설정한 보안등급에 따라야 한다.

(2) 보안등급 1에서 항만시설은 보안사건을 식별하고 예방조치를 시행하기 위하여 ISPS Code B편에 있는 지침을 고려하여 다음 조치들을 시행하여야 한다.

① 항만시설보안 임무를 수행

② 항만시설에의 접근통제

③ 묘박지 및 정박지를 포함하여 모든 항만시설을 모니터링

④ 인가자만이 접근할 수 있도록 제한구역을 감시

⑤ 화물의 취급을 감독

⑥ 선용품 취급을 감독

⑦ 즉각적으로 사용 가능한 보안통신 이용 보장

(3) 보안등급 2에서는 추가보안조치를 수행하여야 하고, 보안등급 3에서는 추가의 특정한 보호조치가 시행되어야 한다.

(4) 보안등급 3에서는 당사국 정부가 지시한 보안지시사항도 추가로 시행하여야 한다.

(5) 선박이 SOLAS 11-2장 또는 ISPS Code A편의 요건을 준수하거나 선박보안계획서에 있는 보안조치들을 시행하는데 애로사항이 있다고 항만시설보안책임자가 통보를 받는 경우 그리고 당사국 정부가 지시

하는 보안지침을 따라야 하는 보안등급 3의 경우에는 항만시설보안책임자와 선박보안책임자가 협조하여 적절한 보안조치를 조정하여야 한다.

(6) 선박의 보안등급이 항만시설의 보안등급보다 더 높은 경우 항만시설보안책임자는 담당 기관에 이를 보고하여야 한다.

15) 항만시설보안평가(제15절)

총 7개 항으로 구성되어 있으며 항만시설보안평가가 시행되어야 하는 시기 및 항만시설보안평가에 포함되어야 하는 사항을 규정하고 있다.

(1) 항만시설보안평가는 항만시설보안계획서 개발 및 최신화 과정에서 필수적인 부분이다.[20]

(2) 항만시설보안평가는 당사국정부에 의해 수행되어야 하며 당사국 정부는 보안인증심사대행기관에게 항만시설보안평가를 위임할 수 있다. 보안인증심사대행기관이 항만시설보안평가를 대행한 경우에는 당사국 정부가 적합성을 검토하고 승인하여야 한다.

(3) 항만시설보안평가는 보안평가를 할 수 있는 적절한 기술이 있는 자가 수행하여야 한다.

(4) 항만시설보안평가는 정기적으로 검토 및 최신화되어야 하고 항만시설에 중대한 변경이 발생한 경우에는 반드시 검토되어 최신화되어야 한다.

(5) 항만시설보안평가는 최소한 다음 요소들을 포함하여야 한다.

① 중요하게 보호되어야 하는 주요 자산 및 기반시설의 식별 및 평가

② 보안조치를 수립하고 우선순위를 결정하기 위하여 자산 및 기반시설에 대하여 일어날 수 있는 위협과 발생 가능성을 식별

③ 취약성을 감소시키기 위한 대응조치 및 절차변경 그리고 그것들의 유효성의 정도를 식별, 선택하고 우선순위를 결정

④ 기반시설, 정책 및 절차에 있어서 인적요소를 포함한 취약점을 식별

(6) 당사국 정부는 항만시설들이 유사한 경우 하나의 항만시설보안평가를 가지고 다수의 항만시설에 적용할 수 있다. 그러한 경우 관련 사항을 국제해사기구에 통보하여야 한다.

(7) 항만시설보안평가가 완료되면 보안평가 방법, 발견된 취약성에 대한

20) 항만시설보안계획서를 개발하고 최신화할 때는 반드시 항만시설보안평가를 시행하고 그 결과를 바탕으로 하여야 한다.

설명 및 취약성을 다루는데 사용될 수 있는 대응조치의 설명 요약이 포함된 보고서가 작성되어야 하며 이 보고서는 무단접근 또는 폭로로부터 보호되어야 한다.

16) 항만시설보안계획서(제16절)

총 8개 항으로 구성되어 있으며 항만시설보안계획서에 포함되어야 하는 사항들에 대하여 규정하고 있다.

(1) 항만시설보안계획서는 항만시설보안평가를 근거로 하여 선박/항만인터페이스를 적절하게 할 수 있도록 각 항만시설에 대하여 개발하고 유지하여야 한다.

(2) 보안인증심사대행기관이 항만시설보안계획서를 준비한 경우 당사국 정부가 승인하여야 한다.

(3) 항만시설보안계획서는 최소한 다음 사항을 포함하여야 한다.

① 사람, 선박 또는 항만에 위협을 주는 무기 또는 위험물질 및 설비 그리고 허가되지 않은 물건이 항만시설 또는 선박에 반입되는 것을 방지하기 위한 조치

② 항만시설, 항만시설에 계류된 선박 및 항만시설의 제한구역으로 무단 접근하는 것을 방지하기 위한 조치

③ 항만시설 또는 선박/항만인터페이스의 중요 작업을 시행하기 위한 규정을 포함하여 보안위협 또는 보안위반에 대응하는 절차

④ 보안등급 3에서 당사국 정부가 지시하는 보안지침을 수용하기 위한 절차

⑤ 보안위협이나 보안위반의 경우에 철수 절차

⑥ 보안측면에서 보안임무가 부여된 항만시설근무자 및 기타 항만시설근무자의 의무

⑦ 선박보안활동과 인터페이스 하는 절차

⑧ 항만시설보안계획서의 정기적인 검토 및 최신화하는 절차

⑨ 보안사건 보고 절차

⑩ 항만시설보안책임자 지정 및 24시간 연락처 설정

⑪ 항만시설보안계획서에 포함된 정보에 대한 보안을 유지하기 위한 절차

⑫ 항만시설에 있는 화물 및 화물취급 장비에 대한 효과적인 보안을 확보하기 위한 절차

⑬ 항만시설보안계획서를 심사하기 위한 절차

⑭ 항만시설에서 선박보안경보시스템이 작동될 경우에 대응하는 절차
⑮ 선원이 상륙할 때 또는 교대할 때뿐만 아니라 선원의 복지 및 노동조합 대표자가 본선을 방문할 때 쉽게 이루어지도록 하는 절차

(4) 내부심사를 하는 자는 심사를 받는 활동으로부터 독립되어야 한다.[21)]

(5) 당사국 정부는 항만시설보안계획서의 내용 중 당사국 정부가 개정사항을 승인하지 않는 한 개정되어 시행되어서는 안 되는 사항[22)]을 결정하여야 한다.

(6) 항만시설보안계획서는 무단 접근 또는 폭로로부터 보호되어야 한다.

(7) 당사국 정부는 항만시설이 유산한 경우 하나의 항만시설보안계획서를 다수의 항만시설에 적용되는 것을 허용할 수 있다. 그러한 경우 당사국 정부는 국제해사기구에 통보하여야 한다.

17) 항만시설보안책임자(제17절)

총 3개 항으로 구성되어 있으며 항만시설보안책임자의 책임과 의무에 대하여 규정하고 있다.

(1) 각 항만시설에는 항만시설보안책임자가 지정되어야 한다. 한 사람이 하나 이상의 항만시설에 대한 항만시설보안책임자로 지정될 수 있다.

(2) 항만시설보안책임자는 다음과 같은 의무와 책임을 갖는다.

① 항만시설보안평가를 고려하여 항만시설에 대한 최초종합적인 보안검사 시행
② 항만시설보안계획서를 개발하고 유지
③ 항만시설보안계획서를 시행하고 연습
④ 적절한 보안조치가 지속적으로 시행되도록 하기 위하여 항만시설에 대한 정기적인 점검 실시
⑤ 결함을 시정하기 위하여 그리고 항만시설에 변화가 있을 때 이를 반영하여 항만시설보안계획서를 최신화시키기 위하여 항만시설보안계획서를 적절히 수정
⑥ 항만시설종사자의 보안의식 및 경계 강화

---

21) 내부심사는 조직(항만시설)이 보안계획서에 따라 보안시스템을 적합하고 효과적으로 수행하고 있는지 조직 스스로 검증하는 프로세스이다. 그러므로 내부심사가 객관적이 되기 위해서는 심사 대상이 되는 업무와 직접적인 연관이 없는 자가 심사를 수행하는 것이 원칙이다. 따라서 조직의 규모나 특성 등으로 인하여 불가능하지 않다면 심사 대상 업무와 독립적인 위치에 있는 자가 내부심사를 수행하여야 한다.

22) 보안상 민감하고 중요하다고 판단되는 사항은 잘못된 방향으로 개정되는 경우에는 보안수준을 감소시킬 수 있으므로 당사국 정부로부터 개정사항을 승인 받은 후에 시행하도록 하여야 한다. 당사국 정부는 이런 사항이 어떤 것인지를 명확히 결정하여야 한다.

⑦ 항만시설에서 보안임무가 있는 인원들에 대한 적절한 교육 시행
⑧ 항만시설의 보안을 위협하는 사건을 관련 당국에 보고하고 기록을 유지
⑨ 선박의 회사 및 선박보안책임자와 항만시설보안계획서 이행에 대하여 협의
⑩ 보안업무에 대하여 협의
⑪ 항만시설에서 보안임무가 있는 인원들에 대한 기준이 만족되도록 보장
⑫ 보안장비가 있는 경우 이에 대한 적절한 작동, 시험, 교정 및 정비 보장
⑬ 요청이 있는 경우 승선하고자 하는 사람의 신원 확인하는데 대하여 선박보안책임자를 지원

(3) 항만시설보안책임자는 SOLAS 11-2장 및 ISPS Code A편에 규정된 의무와 책임을 충실히 수행하기 위하여 필요한 지원을 받아야 한다.

18) 항만시설보안에 관한 교육, 훈련 및 연습(제18절)

총 4개 항으로 구성되어 있으며 항만시설보안책임자 및 특정한 보안임무를 수행하고 있는 인원들에 대한 교육 및 주기적인 훈련과 연습이 시행되어야 함을 규정하고 있다.

항만시설보안책임자, 항만시설보안요원 및 특정한 보안임무를 담당하는 인원은 ISPS Code B편의 지침을 고려하여 충분한 지식을 가져야 하고 적절한 교육을 받아야 한다고 규정하고 있다. 그리고 적절한 간격으로 훈련이 실시되어야 하며 항만시설보안책임자는 적절한 간격으로 연습에 참여하여 항만시설보안계획서가 적절히 시행되도록 보장할 것을 요구하고 있다.

19) 선박의 심사 및 증서발급(제19절)[23]

23) 선박에 대해 시행되는 심사 종류와 발급되는 증서 종류에 대하여는 ISPS Code A편에서 규정하고 있으나, 항만시설에 대해서는 관련 규정이 ISPS Code A편에 규정되어 있지 않다. ISPS Code A편 4절 "당사국 정부의 책임"에는 당사국 정부가 적절한 수준으로 선박 및 항만시설 보안계획서의 유효성을 테스트하도록 규정되어 있으나 후속되는 ISPS Code A편 규정에는 항만시설에 대하여는 구체적인 방법이 제시되어 있지 않다. 이는 선박의 경우에는 다른 당사국 정부의 영토·영해에 들어가기 때문에 선박이 국제협약을 성실히 준수하고 있는지를 나타내는 수단이 필요하고 그 증거가 심사를 받고 증서를 유지하는 것이다. 그리고 이러한 사항은 항만국 통제에서 주요한 확인 대상이 된다. 항만시설의 경우에는 SOLAS협약에서 적용 대상에는 포함시켰지만 항만국 통제와 같은 수단을 통해서 객관적으로 확인을 할 수 있는 수단이 없다. 단지 IMO에 정보를 통보하는 정도

총 4개 항으로 구성되어 있으며 선박에 대해 시행되는 심사의 종류 및 발급되는 증서의 종류, 유효기간과 증서발급 조건 등에 대하여 규정하고 있다.

(1) 선박 심사의 종류

① 최초심사(Initial verification) : 증서[24]를 최초로 발급하기 전에 시행하는 심사

② 갱신심사(Renewal verification) : 증서 유효기간이 만료되어 새로운 증서를 발급하기 위한 심사

③ 중간심사(Intermediate verification) : 최초심사와 갱신심사 사이에 시행하는 심사로서 만약 단 한번의 중간심사만 시행된다면 두 번째 연차일(anniversary date)과 세 번째 연차일 사이에 시행되어야 함.

④ 추가심사(Additional verification) : 주관청이 필요하다고 인정한 경우에 추가로 시행하는 심사

(2) 증서

① 증서 발행 : 최초심사 및 갱신심사 후에 발행

② 증서 유효기간 : 5년을 초과하지 아니하는 기간으로 주관청이 설정

③ 증서 이서 : 중간심사 후에 이서

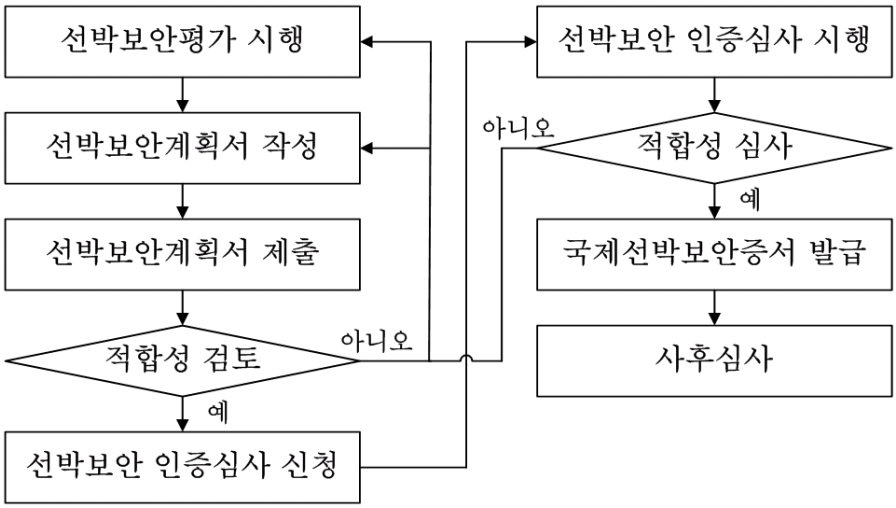
④ 증서 효력 정지 : 해당되는 심사가 시행되지 않은 경우, 운항책임을 맡은 회사가 변경된 경우, 선박의 기국이 변경된 경우에 증서는 효력이 정지

(3) 선박의 보안시스템 수립 및 인증 과정

일 뿐이다. 그러므로 항만시설에 대한 심사 및 증서 발급은 전적으로 항만시설이 속한 당사국 정부의 책임 및 권한으로 이루어진다. 그렇기 때문에 강제적으로 적용되는 규정인 ISPS Code A편에서 그 내용을 언급하는 것이 부적절하기 때문에 포함되어 있지 않다고 볼 수 있다. 여기에 대한 지침은 ISPS Code B편의 부록에 제시된 항만시설 적합확인서 서식에 내용이 제시되고 있다.

24) 증서란 국제선박보안증서(International Ship Security Certificate, ISSC)를 말한다.

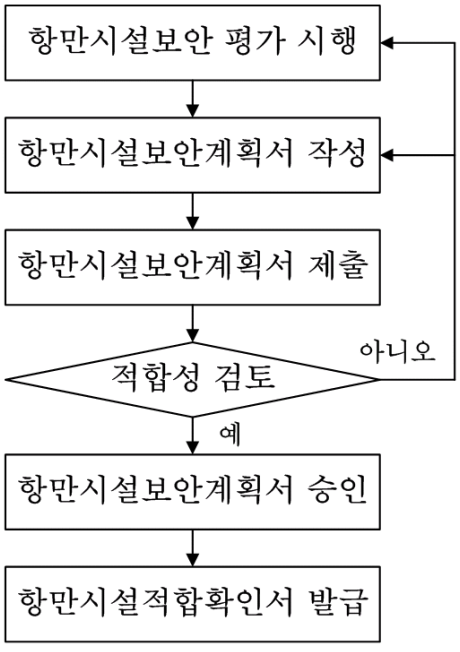
<그림 2-1> 선박의 보안시스템 수립 및 인증 과정



주) ISPS Code A편, B편을 근거로 필자가 정리하였음.

(4) 항만시설의 보안시스템 수립 및 인증 과정

<그림 2-2> 항만시설의 보안시스템 수립 및 인증 과정



주) ISPS Code A편, B편을 근거로 필자가 정리하였음.

4. ISPS Code B편의 내용

ISPS Code B편은 SOLAS 11-2장 및 ISPS Code A편에 규정된 강제 요건을 준수하기 위한 구체적인 실행 방법에 대하여 규정하고 있다.

강제적 적용 사항인 ISPS Code A편에 대한 구체적인 적용 요건 및 설명을 전개시켜나가고 있다. 구성은 ISPS Code A편의 구성과 동일하게 되어 있어서 A편에 해당되는 지침을 찾고자 할 때 쉽게 확인될 수 있도록 되어 있다(<표 2-4> 참조).

ISPS Code B편은 강제적으로 이행하여야 하는 요건은 아니다. 그래서 표현을 할 때도 무엇을 하여야 한다가 아니라 어떻게 할 수도 있다는 식의 표현으로 전개되고 있다. 그러나 실제로 SOLAS 11-2장의 요건 및 ISPS Code A편에 규정된 요건을 이행하고자 할 때는 ISPS Code B편에 규정된 지침을 반영하지 않고는 이행이 불가능하다. 그러므로 최소한의 이행 요건으로 ISPS Code B편의 지침을 반영하지 않을 수 없다. 이런 이유 때문에 국제해사기구에서는 선박 보안시스템을 수립할 때는 해당되는 부분의 지침을 강제적으로 반영하여야 한다고 별도의 문서를 채택하여 규정하고 있다. 항만시설의 경우에는 강제로 적용하여야 한다는 별도 규정은 없지만 앞에서도 언급한 것과 같이 보안시스템을 수립하고 유지하기 위해서는 B편의 내용을 준수하지 않을 수 없다고 판단된다.

<표 2-4> ISPS Code B편의 세부 조항

번호	ISPS Code A편, B편 조항	ISPS Code B편 세부조항
1	개 요	- 일반사항(1.1-1.5) - 당사국 정부의 의무(1.6-1.7) - 보안등급의 설정(1.8) - 회사와 선박(1.9-1.15) - 항만시설(1.16-1.21) - 정보 및 정보교환(1.22)
2	정 의	- 용어의 정의(2.1-2.2)
3	적 용	- 일반사항(3.1-3.4)
4.	당사국 정부의 책임	- 평가 및 계획의 보안(4.1) - 지정당국(4.2) - 보안인증심사대행기관(4.3-4.7) - 보안등급의 설정(4.8-4.13) - 항만시설보안계획서에 관한 정보 및 연락처(4.14-4.17) - 신원확인문서(4.18) - 고정식 및 부유식 플랫폼 그리고 작업중인 이동식 해상 구조물(4.19) - ISPS Code A편의 적용이 요구되지 않는 선박(4.20) - 선박에 대한 위협 및 해상에서의 기타 사고(4.21-4.25) - 대체 보안 협정문(4.26) - 항만시설에 대한 동등한 조치(4.27) - 인력배치의 수준(4.28) - 통제 및 적합조치(4.29-4.46)
5	보안선언서	- 일반사항(5.1-5.6)
6	회사의 의무	- 일반사항(6.1-6.8)
7	선박보안	- 세부조항 없음

<표 2-4> ISPS Code B편의 세부 조항(계속)

번호	ISPS Code A편, B편 조항	ISPS Code B편 세부조항
8	선박보안평가	- 보안평가(8.1-8.13) - 현장보안검사(8.14)
9	선박보안계획서	- 일반사항(9.1-9.6) - 선박보안임무의 조직 및 수행(9.7-9.8) - 선박에 대한 접근(9.9-9.17) - 선박에서의 제한구역(9.18-9.24) - 화물의 취급(9.25-9.32) - 선용품의 인도(9.33-9.37) - 미휴대 수화물의 취급(9.38-9.41) - 선박보안 모니터링(9.42-9.49) - 보안등급의 차이(9.50) - ISPS Code가 적용되지 않는 대상과의 활동(9.51) - 보안선언서(9.52) - 심사 및 검토(9.53)
10	기록	- 일반사항(10.1-10.2)
11	회사보안책임자	- 세부조항 없음
12	선박보안책임자	- 세부조항 없음
13	선박보안에 관한 교육, 훈련 및 연습	- 교육(13.1-13.4) - 훈련 및 연습(13.5-13.8)
14	항만시설보안	- 세부조항 없음

<표 2-4> ISPS Code B편의 세부 조항(계속)

번호	ISPS Code A편, B편 조항	ISPS Code B편 세부조항
15	항만시설보안평가	- 일반사항(15.1-15.4) - 중요하게 보호되어야 하는 주요자산 및 기반시설의 식별 및 평가(15.5-15.8) - 보안조치의 우선순위를 정하기 위한 자산 및 기반시설에 대한 예상 위협 및 발생가능성의 식별(15.9-15.12) - 취약성을 감소시키기 위한 대응방안, 절차의 변경 및 유효성 수준에 대한 식별, 선별 및 우선순위의 결정(15.13-15.14) - 취약성의 식별(15.15-15.16)
16	항만시설보안계획서	- 일반사항(16.1-16.7) - 조직 및 항만시설보안임무의 수행 (16.8-16.9) - 항만시설에의 접근(16.1016.20) - 항만시설내의 제한구역(16.21-16.29) - 화물의 취급(16.30-16.37) - 선용품의 인도(16.38-16.44) - 미휴대 수화물의 취급(16.45-16.48) - 항만시설의 보안 모니터링(16.49-16.54) - 보안등급의 차이(16.55) - ISPS Code가 적용되지 않는 활동(16.56) - 보안선언서(16.57) - 심사, 검토 및 개정(16.58-16.60) - 항만시설보안계획서의 승인(16.61) - 항만시설 적합확인서(16.62-16.63)
17	항만시설보안책임자	- 일반사항(17.1-17.2)
18	항만시설보안에 대한 교육, 훈련 및 연습	- 교육(18.1-18.3) - 훈련 및 연습(18.4-18.6)
19	선박의 심사 및 증서 발급	- 세부조항 없음

ISPS Code B편의 세부조항 중에서 항만시설 보안시스템과 관련된 부분을 요약하면 다음과 같다.

1) 개요(제1항)

(1) 일반사항

ISPS Code B편의 내용은 항만시설 내에 선박이 있을 대 선박을 보호하는 것과 우선적으로 연관이 있다. 그러나 선박이 항만시설에 위협을 줄 수도 있다. 왜냐하면 선박이 항만시설 내에 있게 되면 공격을 개시하기 위한 기지로 사용될 수 있기 때문이다. 선박을 기지로 한 보안위협에 대응하기 위한 적절한 보안수단을 고려할 때 항만시설 보안평가와 항만시설보안계획서 작성은 이 지침을 고려하여야 한다.

(2) 당사국 정부의 의무

① 자국 영토 내에 있는 항만시설 중에서 항만시설보안계획서를 수립할 책임을 지는 항만시설보안책임자의 지정이 요구되어지는 항만시설을 결정

② 항만시설보안평가의 완료, 승인 및 이미 승인된 평가의 후속개정사항의 승인

③ 항만시설보안계획서 및 이미 승인된 동 계획서의 후속개정사항을 승인

④ 승인된 계획서에 테스트 실시

당사국 정부는 항만시설과 관련된 특정업무를 수행하는 것을 항만시설보안인증심사대행기관에 위임할 수 있다. 그러나 최종 승인은 당사국 정부가 하여야 한다. 그리고 어떤 업무는 위임할 수 없으며 반드시 당사국 정부가 수행하여야 한다(<표 2-5> 참조).

<표 2-5> 당사국 정부가 직접 수행하여야 하는 보안업무
(항만시설 보안관련)

- 보안등급 설정
- 항만시설보안책임자 지정, 항만시설보안계획서를 작성해야 되는 항만시설 결정
- 항만시설보안평가 승인 (개정 사항에 대한 승인 포함)
- 항만시설보안계획서 승인 (개정 사항에 대한 승인 포함)
- 보안선언서의 요건 수립

(3) 보안등급의 설정

항만시설에 적용하기 위한 보안등급을 설정하여야 하며 국제적으로 동일한 체계로 적용하기 위하여 3등급으로 보안등급을 구분한다.

(4) 항만시설

① 항만시설보안평가는 주기적으로 검토되어야 한다.

② 보안위험성은 표적에 노출될 취약성 및 공격의 결과가 결합된 공격위협의 함수 작용이다.

③ 보안평가는 다음 요소들을 반드시 포함하여야 한다.

- 항만시설 및 기반시설에 대하여 예견되는 위협을 반드시 결정
- 잠재적 취약성 식별
- 사고결과 추산

2) 적용(제3항)

군사용으로 설계 및 사용되는 항만시설에는 적용하지 않는다.

3) 보안선언서(제5항)

(1) 일반사항

① 보안선언서는 항만시설의 당사국 정부가 또는 선박이 필요하다고 간주할 때 완성되어져야 한다.

② 보안선언서가 필요한지 여부는 항만시설보안평가 결과로 나타날 수 있으며 보안선언서가 요구되는 이유 및 상황은 항만시설보안계획서에 설정되어 있어야 한다.

③ 선박 또는 선박의 대신하여 선박의 주관청이 보안선언서 작성을 요청하는 경우 항만시설보안책임자 또는 선박보안책임자는 그런 요청을 인지하고 타당한 보안조치들을 논의하여야 한다.

④ 항만시설보안책임자는 특별한 주의가 필요한 것이라고 승인된 항만시설보안계획서에 식별되어 있는 선박/항만인터페이스는 선박/항만인터페이스를 시행하기에 앞서서 보안선언서를 제안할 수 있다.

⑤ 보안선언서의 주요 목적은 각자의 보안계획서에 따라 시행하는 보안조치에 대하여 인터페이스 하는 선박과 항만시설 간 또는 선박과 다른 선박 간에 합의가 이루어졌음을 나타내기 위한 것이다.

⑥ 합의된 보안선언서는 항만시설보안책임자와 선박보안책임자 양측의 서명이 있어야 한다.

4) 항만시설보안평가(제15항)

(1) 일반사항

항만시설보안평가는 항만시설 내 다음 요소들을 다루어야 한다.

① 물리적 보안

② 구조 완전성

③ 개인보호 시스템

④ 절차상의 방법

⑤ 무선 및 원격통신시스템(컴퓨터 시스템 및 네트워크 포함)

⑥ 운송 관련 기반시설

⑦ 설비

⑧ 만약 파괴되거나 불법정탐에 사용되는 경우 항만시설내의 인명, 재산 또는 운영에 위험성이 있는 기타 분야

(2) 중요하게 보호되어야 하는 주요자산 및 기반시설 식별 및 평가

항만시설의 기능 유지 측면에서 주요자산 및 기반시설의 상대적 중요성을 판단하기 위한 프로세스이다.

보안사건으로부터 어떤 자산 및 설비를 더 중요하게 보호해야 하는지를 판단할 수 있는 기본적인 자료를 제공한다. 판단할 때 인명손실에 대한 부분을 우선적으로 고려하여야 하며 경제적 중요성, 상징적 가치, 정부 시설 유무 등을 고려하여야 한다.

또한 주요자산이나 기반시설이 없더라고 항만시설, 구조물 또는 설비들이 정상작동이 가능한지 그리고 정상기능이 가능하도록 하기위한 신속한 복구 범위 등을 고려하여야 한다.

중요하게 보호되어야 할 자산 및 기반시설은 다음과 같은 것들을 포함한다.

① 통행로, 출입구, 접근로, 묘박지, 선박 조종 지역, 접안 지역

② 화물 설비, 터미널, 화물 보관구역, 화물 취급 장비

③ 전기 배선 시스템, 무선 및 원격통신시스템, 컴퓨터 시스템, 네트워크

④ 항내 선박 통항 관제 시스템 및 항로표지

⑤ 발전소, 화물 이송 파이프, 수도 시설

⑥ 교량, 철도, 도로

⑦ 항내 서비스 선박(도선선, 예인선, 부선 등)

⑧ 보안 및 감시 장비와 시스템

⑨ 항만시설에 인접한 수역

(3) 보안 조치의 우선순위를 정하기 위한 자산 및 기반시설에 대한 예상 위협 및 발생가능성의 식별

주요 자산 및 장소에 대한 취약성을 평가하고 계획 수립과 자원 분배가 가능하도록 보안요건의 우선순위를 수립하기 위하여 주요 자산과 기반시설의 보안에 위협을 줄 수 있는 행위 및 그러한 행위가 실행되도록 하는 방법이 무엇인지 식별하여야 한다.

다음과 같은 보안사건 들을 포함하여 모든 가능한 보안위협에 대하여 고려하여야 한다.

① 항만시설 또는 선박의 파괴
② 선박 또는 선박에 승선한 인원의 납치 또는 강탈
③ 화물, 선박의 주요 설비 및 시스템 또는 선용품에 대한 조작
④ 밀항자를 포함한 불법 출입 또는 불법 이용
⑤ 대량살상무기를 포함한 무기 및 장비의 밀수
⑥ 보안사건을 일으킬 수 있는 사람들이나 그들의 장비를 이송하기 위한 선박 이용
⑦ 손상 또는 파괴수단 또는 무기로서 선박자체 사용
⑧ 항만 입구, 갑문, 접근로 등의 봉쇄
⑨ 핵, 생화학 공격

(4) 취약성을 감소시키기 위한 대응방안, 절차의 변경 및 유효성 수준에 대한 식별, 선별 및 우선순위 결정

대응방안 식별 및 우선순위 결정은 항만시설 또는 선박/항만 인터페이스에서 발생 가능한 위협에 대한 취약성을 줄이기 위하여 가장 효과적인 보안조치가 도입되도록 하는 것이다.

(5) 취약성 식별

취약성 식별은 취약성을 제거하거나 완화시키는 방법을 수립하기 위하여 필요하다.

취약성 식별에는 다음 사항이 고려되어야 한다.

① 항만시설 및 항만시설에 계류 중인 선박에 대한 해상 측과 육상 측으로부터의 접근
② 부두, 항만시설 및 관련 구조물들의 구조완전성
③ 신원확인시스템을 포함한 현행 보안 방법 및 절차
④ 항만서비스 및 시설에 관한 현행 보안조치 및 절차
⑤ 컴퓨터 시스템 및 네트워크를 포함한 무선 및 원격통신설비, 항만서비스 및 시설을 보호하기 위한 조치

⑥ 공격 중 또는 공격을 위하여 이용될 수 있는 주변지역
⑦ 해상/육상 측의 보안서비스를 제공하고 있는 보안회사와의 합의 사항
⑧ 안전과 보안조치 및 절차들 간에 상충되는 수단
⑨ 항만시설 및 보안임무 배치에서 상충되는 부분
⑩ 법률의 집행 및 인신의 구금
⑪ 교육 및 훈련 중 식별된 결함사항
⑫ 일상 업무, 사건이나 경보 후속, 보안관련 보고, 통제조치의 연습, 심사 등에서 발견된 결함사항

5) 항만시설보안계획서(제16항)

(1) 일반사항

항만시설보안계획서를 작성하는 것은 항만시설보안책임자의 책임이다. 항만시설보안계획서에는 다음 사항들이 포함되어야 한다.

① 항만시설의 보안조직에 대한 상세사항
② 보안조직과 관련 당국과의 연계 및 통신시스템
③ 보안등급 1에서의 보안조치 상세사항
④ 보안등급 2 또는 필요한 경우 보안등급 3으로 지체 없이 변경하기 위한 부가적인 보안조치
⑤ 항만시설보안계획서의 규칙적 검토, 심사 및 개정 절차
⑥ 당사국 정부에 대한 보고절차

당사국 정부는 항만시설보안계획서를 승인하여야 한다.

(2) 조직 및 항만시설보안임무의 수행

항만시설보안계획서에는 항만시설 근무자의 임무와 책임 그리고 항만시설이 수행하는 보안임무에 대하여 각 보안등급별로 수립하여야 한다.

(3) 항만시설에의 접근

항만시설보안계획서에는 항만시설보안평가에서 식별된 항만시설로 접근하기위한 모든 수단에 대응하는 보안조치를 수립하여야 한다. 이를 위해서 접근제한 또는 접근금지를 적용하여야 하며 적용될 종류를 구체화하여야 한다. 각 개인에 대하여는 신원확인 수단을 각 보안등급별로 수립하여야 한다.

(4) 항만시설내의 제한구역

항만시설보안계획서에는 항만시설 내에 지정되는 제한구역을 식별하여야 하고 범위, 적용 시간, 제한구역 접근 통제를 위해 취해져야 하는 보안조치 및 제한구역 내에서의 활동을 통제하기 위해 취해져야

하는 보안조치를 구체적으로 나타내어야 한다. 항만시설보안계획서에는 모든 제한구역이 접근이 제한되어 있으며 관계자 이외의 접근은 보안을 위반하게 됨을 명확히 나타내도록 하는 것을 포함하여야 한다.

(5) 화물의 취급

화물 취급과 관련된 보안조치들은 화물조작을 방지하고, 운송예정이 없는 화물이 항만시설 내로 받아들여지거나 보관되는 것을 방지하도록 하여야 한다.

(6) 선용품 인도

선용품의 인도와 관련된 보안조치들은 다음과 같다.

① 선용품 및 포장상태의 점검

② 검사를 받지 않고 선용품이 전달되는 것을 방지

③ 조작 방지

④ 주문하지 않은 선용품이 전달되는 것을 방지

⑤ 선용품 배달 차량 검색

⑥ 항만시설 내에서 배달 차량 호위

(7) 미휴대 수화물의 취급

항만시설보안계획서에는 미휴대 수화물[25]을 항만시설 내로 들여오기 전에 그리고 항만시설에서 선박으로 이동하기 전에 검색을 포함한 스크리닝(screening)이 실시됨을 나타내어야 한다.

(8) 항만시설의 보안모니터링

항만시설의 보안조직은 야간 및 시계에 제한이 있는 기간을 포함하여 항시 육지와 수면 상의 항만시설과 인근 진입장소, 항만시설의 제한구역, 항만시설에 정박해 있는 선박과 선박을 둘러싸고 있는 지역들을 감시하는 능력을 갖추어야 한다.

(9) 보안등급의 차이

항만시설보안계획서에는 항만시설의 보안등급이 선박의 보안등급보다 낮은 수준인 경우 항만시설이 채택할 수 있는 절차 및 보안조치들의 세부사항을 수립하여야 한다.

(10) ISPS Code가 적용되지 않는 대상과의 활동

항만시설보안계획서에는 다음과 같은 경우 항만시설이 적용해야 하는 절차 및 보안조치의 세부사항을 수립하여야 한다.

---

25) 미휴대 수화물은 검색(inspection) 또는 수색(search) 하는 곳에서 여객 또는 선박 승무원이 휴대하고 있지 않은 수화물로 개인소지품도 포함한다.

① 당사국 정부가 아닌 국가의 항만에 있었던 선박과 인터페이스를 하고 있는 경우
② ISPS Code 적용을 받지 않은 선박과 인터페이스를 하고 있는 경우
③ 작업 중인 고정 또는 부유식 플랫폼 또는 이동식 해상 구조물(MODU)과 인터페이스를 하고 있는 경우

(11) 보안선언서

항만시설보안계획서에는 항만시설보안책임자가 보안선언서를 요청할 때 또는 선박이 보안선언서를 요청할 때 조치하는 절차를 수립하여야 한다.

(12) 심사, 검토 및 개정

항만시설보안계획서에는 항만시설보안책임자가 심사를 시행하는 절차와 항만시설보안계획서를 검토, 최신화 또는 개정하기 위한 절차를 수립하여야 한다.

(13) 항만시설보안계획서의 승인

항만시설보안계획서에는 다음 사항에 대한 절차를 수립하여야 한다.
① 항만시설보안계획서를 당사국 정부에 제출
② 항만시설보안계획서 심의
③ 항만시설보안계획서 승인(수정 또는 수정 없이)
④ 승인 후의 개정사항에 대한 심의
⑤ 승인된 항만시설보안계획서의 지속적인 타당성을 심사 또는 검사하기 위한 절차

(14) 항만시설 적합확인서

당사국 정부는 항만시설에 대해 다음 사항을 나타내는 항만시설 적합확인서를 발행할 수 있다.
① 항만시설
② 항만시설이 SOLAS 제11-2장 및 ISPS Code A편을 만족함
③ 유효기간(5년을 넘을 수 없음)
④ 사후심사 확인

6) 항만시설보안책임자(제17항)

공식적인 목적으로 선박에 승선하려고 하는 사람의 신원 확인 문서의 유효성에 대해 선박보안책임자가 문의하는 경우에는 항만시설보안책임자는 이에 대해 지원하여야 한다.

7) 항만시설보안에 대한 교육, 훈련 및 연습(제18항)

(1) 교육

항만시설보안책임자, 특정의 보안임무를 맡은 항만시설 근무자, 기타 모든 항만시설 근무자는 자신이 해당되는 부분에 대한 지식이 있어야 하며 필요한 교육을 받아야 한다.

(2) 훈련 및 연습

훈련 및 연습의 목적은 모든 보안등급에서 항만시설근무자가 부여된 보안임무를 능숙하게 수행하도록 하고, 보안관련 결함들을 식별하는 것이다.

제3장 항만시설 보안평가 모델 구축

항만시설 보안평가는 항만시설 보안시스템을 수립하는데 있어서 가장 기초가 되는 부분이며 필수적인 과정이다. 항만시설 보안평가가 정확하게 수행되지 않으면 효과적이고 ISPS Code에 적합한 항만시설 보안시스템이 수립될 수 없다. 그러므로 항만시설 보안시스템을 성공적으로 수립하기 위해서는 체계적인 방법론을 적용하여 항만시설 보안평가를 시행하여야 할 것이다. 본 장에서는 항만시설 보안평가에 대한 방법론을 구축하기 위한 이론적인 모델로서 위험성 평가 방법을 설정하고 이에 대하여 고찰해본다. 그리고 위험성 평가 방법론을 근거로 항만시설 보안평가를 수행하는 방법론을 모색하여 구체적인 항만시설 보안평가 모델을 설정하고자 한다.

제1절 위험성 평가 분야의 선정

위험성 평가에 대한 이론적인 전개를 하기 위해서는 대상으로 삼고자하는 위험성의 범주를 명확히 설정할 필요가 있다. 즉 어떤 분야의 위험성에 대하여 위험성 평가 방법론을 고찰할 것인지를 정확히 규정하여야 한다.

오늘날 위험성 또는 리스크(Risk)라는 용어는 다양한 분야에서 사용되고 있다. 국가 경영, 기업 경영 또는 개인적인 생활에서도 우리는 위험성이라는 용어를 사용하고 있다. 또 조금 더 세부적으로 구분해보면 기업 경영의 경우에 재무적인 부분에서의 리스크, 안전 분야에서의 리스크, 환경 부분에서의 리스크, 보안 분야에서의 리스크 등과 같이 여러 분야에 걸쳐서 위험성이라는 용어를 사용하고 있다. 이와 같이 지금은 여러 부문에 걸쳐 위험성이라는 개념이 보편화되어 적용되고 있다. 그러나 본래 이 개념은 산업재해를 예방하기 위한 안전을 다루는 분야에서 출발하였다고 볼 수 있다.

작업장에서는 다양한 원인으로 말미암아 사건이나 사고가 발생하게 된다. 그리고 이러한 사건이나 사고 중 많은 부분은 인적 또는 물적 피해를 일으키게 된다. 인적 또는 물적 피해가 발생하면 기업은 이로 인하여 직접적인 보상 또는 복구비용을 지출하여야 하며 또한 작업 일정이 계획대로 진행되지 않을 것이고 결과적으로 고객에게는 계약사항을 지킬 수 없게 될 수도 있으며 나아가서는 기업의 대외 이미지에도 손상을 입게 된다. 기업의 입장에서는 이런 모든 것들이 유무형의 손실된다. 기업이 유무형의 손실을 입게 되면 이는 기업의 경쟁력이 약화될 것이며 결과적으로 기업의 존폐에도 영향을 미칠 것이다. 그러

므로 기업의 입장에서는 타 기업과의 경쟁에서 우위의 경쟁력을 확보하고 지속적인 발전을 하기 위해서는 손실을 없애거나 줄이기 위한 방법을 찾아야 할 필요성이 있다고 할 수 있다.

인적 또는 물적 피해로 인하여 발생하는 손실을 없애거나 줄이려면 사건이나 사고를 예방하여야 한다. 사건이나 사고를 예방하기 위해서는 이를 발생시키는 다양한 원인을 찾아내서 제거하여야 하며 만약 원인의 완전한 제거가 불가능할 경우에는 사건이나 사고로 진전되지 않도록 하기위한 적절한 관리 방법을 찾아야 한다.

이와 같이 안전을 확보하기 위해서는 사건이나 사고를 발생시키는 다양한 원인인 위험요인을 파악하는 것부터 파악된 원인을 관리하기 위한 방법을 모색하는 것까지 전체적으로 분석하고 접근하여야 할 필요성이 있으며 전체적인 분석과 접근을 위해서는 구체적인 기술적인 방법이 필요하다. 여기에 대한 기술적 사항을 제공하는 것이 위험성 평가 방법이다.[26]

사건이나 사고로부터 야기되는 피해 발생 예방이라는 관점에서 안전과 보안은 동일한 측면을 가지고 있으므로 본 연구에서 고찰하고자 하는 위험성은 안전과 관련된 위험성을 대상으로 선정하여 조명하고자 한다.

제2절 위험성 평가에 연관된 개념들에 대한 정의

위험성 평가를 전개시키기 위해서는 위험성 평가와 관련된 개념들을 파악하고 이들 개념들에 대한 정확한 의미를 규명하여야 한다.

안전과 위험성에 관련된 개념에 대하여는 여러 가지 의미로 정의되어 있으나 본 연구에서는 전 세계적으로 다양한 업종의 사업장에 대하여 안전보건경영시스템 인증규격으로 활용되고 있는 OHSAS 18001[27] 규격을 기준으로 전개

---

26) 한국산업안전공단(Korea Occupational Safety & Health Agency, KOSHA)의 안전보건 일반지침인 안전보건 경영시스템 구축에 관한 지침(KOSHA Code G-04-2003, 공표일 2003. 12. 31.). 부록 2 위험성 평가의 목적에 규정되어 있음. 이 안전보건 경영시스템 구축에 관한 지침은 산업안전보건법 제4조, 동법 시행령 제3조의 2 및 제47조의 규정에 의해 사업장의 자율적인 안전보건경영시스템 구축을 확대 보급하고 사업장내 자율안전 활동의 원활한 운영을 위한 기준을 제공하기 위하여 KOSHA Code로 제정된 것이다.

27) OHSAS 18001은 Occupational Health and Safety Assessment Series 18001로서 작업장의 보건 및 안전에 대한 경영시스템 인증규격이다. 이 규격은 영국표준협회인 BSI의 주도로 전 세계 13개 인증기관 및 표준기관들이 참여하여 제정하였으며 1999년에 공식적으로 공표하였다. OHSAS 18001을 국제표준화기구(ISO)의 규격으로 공표하기 위하여 1996년 11월과 2000년 4월 두 차례에 걸쳐서 투표를 실시하였으나 ISO 회원국들의 반대가 찬성보다 약간 우세하여 국제표준화 규격으로 공표하는 데는 실패하였다. OHSAS 18001이 국제표준화규격으로 채택되는데 실패하였으나 이 규격을 제정한 BSI를 포함한 13개 인증기관 및 표준기관들은 이 규격을 적용하여 안전보건경영시스템에 대한 인증을

하고자 한다.

먼저 안전(Safety)에 대하여는 다음과 같이 정의되어 있다.

“수용할 수 없는 피해의 위험성으로부터 자유로운 것”[28)]

이를 상세히 분석하면 다음과 같은 의미로 이해할 수 있다. 안전은 피해가 발생하지 않도록 하거나 피해가 발생하더라도 수용할 수 있는 범위 즉 인내의 한계 내에 있도록 하면 안전하다는 의미로 볼 수 있다.

수용할 수 없는 피해의 위험성으로부터 자유로운 것을 안전이라고 하였으므로 안전이라는 것을 보다 더 명확히 이해하려면 위험성에 대한 이해가 뒤따라야 한다.

위험성(Risk)은 다음과 같이 정의되어 있다.

“특정한 위험 사건(Hazardous event)이 발생할 가능성(likelihood)과 결과(consequence)의 조합(combination)”[29)]

또 다른 지침에서는 위험성을 다음과 같이 정의하고 있다.[30)]

″특정한 위험요인(Hazard)이 위험한 상태로 노출되어 특정한 사건(Incident)으로 이어질 수 있는 가능성(발생빈도)과 결과의 중대성(손실크기)의 조합으로서 위험의 크기 또는 위험의 정도를 말한다. “

위험성 즉 위험의 크기 또는 위험의 정도를 결정하기 위해서는 위험(Hazard)이 존재하여야 하며 사건(Incident)으로 진전되는 것을 전제로 하여야 한다는 것을 알 수 있다.

여기서 다시 위험(Hazard)과 사건(Incident)에 대한 정확한 의미를 규정할 필요가 있다.

위험(Hazard)은 다음과 같이 정의되어 있다.

“인간의 부상 또는 건강상 장해, 재산상 손해, 작업장 환경에의 손해 또는 이들을 복합적으로 발생시킬 피해 잠재력이 있는 상태 또는 요인”[31)]

하고 있다. 우리나라도 2001년 4월에 ISO 9001과 ISO 14001에 관하여 인정기관 역할을 하고 있는 한국인정협회(KAB, 현 한국인정원) 단체규격인 K-OHSMS 18001 규격으로 등록하였다. 안전보건경영시스템 도입의 필요성을 인식하고 인증 제도를 도입한 많은 국가들은 안전보건경영시스템 표준 규격으로 OHSAS 18001을 채택하고 있다. 그러므로 현재 안전보건경영시스템 인증규격으로 가장 많이 적용되고 있는 것이 OHSAS 18001 규격이다. 그 결과 이 규격은 국제표준화기구의 공식 규격은 아니지만 실질적으로 국제 표준의 역할을 하고 있으므로 ISO 9001이나 ISO 14001과 같은 성격의 규격으로 인식되고 있다.

28) OHSAS 18001:1999 /K-OHSMS 18001:2001 용어의 정의 3.16항.

29) OHSAS 18001:1999 /K-OHSMS 18001:2001 용어의 정의 3.14항.

30) 안전보건 경영시스템 구축에 관한 지침. 3.용어의 정의 (아) (KOSHA Code G-04-2003).

31) OHSAS 18001:1999 /K-OHSMS 18001:2001 용어의 정의 3.4항.

즉 위험이란 인적피해, 물적 손실 및 환경피해를 일으키는 요인 또는 이들 요인이 혼재된 잠재적 유해·위험요인으로 다시 말하면 위험이란 사람·재산 또는 환경에 나쁜 영향을 미치는 어떤 특성이라고 할 수 있다. 이런 특성들이 실제 사고로 진전되기 위해서는 이들 특성들을 움직이게 하는 어떤 자극이 필요하며 이런 자극으로는 기계적 고장, 불안정한 시스템 상태, 작업자의 실수 등과 같은 것이다.

사건(Incident)은 다음 의미로 정의되어 있다.

"사고를 발생시키거나 사고로 이어질 가능성이 있는 사상(事象, event)"[32]

사건이 성립되기 위해서는 사상(event)이 발생하여야 한다. 이 사상은 위험(hazard)이 사고로 진전되도록 움직이게 하는 자극이 된다. 그러므로 사건은 사람·재산 또는 환경에 나쁜 영향을 미치는 어떤 특성이 자극을 받아서 진전되어진 상태를 의미한다. 그리고 사건은 사고를 발생시키거나 사고로 이어질 가능성이 있는 사상 모두이므로 다시 말하면 사건 중에서 일부는 사고로 진전되고 사고로 진전되지 않는 것은 그냥 사건으로 존재한다고 볼 수 있다. 그러므로 사건은 사고를 포함하는 범위로 볼 수 있다.

사고(Accident)는 다음과 같이 정의되어 있다.

"사망, 건강상 장해, 부상, 손해 기타 손실을 발생시키는 의도하지 않은 사상(事象, event)"[33]

즉 사고가 되려면 직접적인 손실이 발생하여야 하며 바라는 행위가 아니어야 한다. 사건 중에서 직접적인 손실이 발생한 부분은 사고에 포함되며 그렇지 않은 부분은 단순한 사건의 범주에 포함된다.

위험성을 이해하고 정의하기 위하여 필요한 개념인 위험, 사건 그리고 사고에 대한 사항을 규정하였다. 다음으로 위험성을 이해하기 위하여 필요한 부분은 '발생 가능성과 결과의 조합'이라는 부분이다. 이는 사건이 발생할 가능성 즉 발생빈도와 사건이 발생했을 때 나타나는 결과 즉 손실의 크기를 결합하여 위험의 크기 또는 위험의 정도인 위험성을 결정하는 것을 의미한다.

위험성 평가는 다음과 같이 정의된다.

"위험성의 크기를 추정하고, 그 위험성이 허용가능한지를 결정하는 전체 프로세서"[34]

위험성의 크기를 추정한다는 것은 위험(Hazard)이 진전되어 사고로 발전될 수 있는 빈도와 손실 크기를 판단하여 위험성 정도를 결정하는 것이며, 위험성

32) OHSAS 18001:1999 /K-OHSMS 18001:2001 용어의 정의 3.6항.

33) OHSAS 18001:1999 /K-OHSMS 18001:2001 용어의 정의 3.1항.

34) OHSAS 18001:1999 /K-OHSMS 18001:2001 용어의 정의 3.15항.

이 허용가능한지를 결정하는 것은 빈도와 손실크기를 조합하여 추정한 위험성이 수용할 수 있는 범위 내 즉 안전 범위 내에 있는지 그렇지 않으면 그 범위를 벗어나는 것인지를 판단하는 것이다.

위에서 정의된 위험성 평가와 관련된 개념들을 표로 정리하면 다음과 같다(<표 3-1> 참조).

<표 3-1> 위험성 평가에 연관된 개념들에 대한 정의

개 념	정 의	의 미
사 고	사망, 건강상 장해, 부상, 손해 기타 손실을 발생시키는 의도하지 않은 사상	사건 중에서 직접적인 손실이 발생한 사건을 말함.
안 전	수용할 수 없는 피해의 위험성으로부터 자유로운 것	위험성의 정도가 인내의 한계 내에 있는 상태를 말함. 즉 위험성이 없거나 위험성이 있더라도 아주 낮은 상태에 있는 것을 말함.
위 험	인간의 부상 또는 건강상 장해, 재산상 손해, 작업장 환경에의 손해 도는 이들을 복합적으로 발생시킬 피해 잠재력이 있는 상태 또는 요인	사람·재산 또는 환경에 나쁜 영향을 미치는 어떤 특성이며 이들 특성이 사고로 진전되기 위해서는 어떤 자극이 필요함.
사 건	사고를 발생시키거나 사고로 이어질 가능성이 있는 사상	손실이 발생한 사상과 손실이 발생하지 않은 사상 모두를 포함하며 위험이 어떤 자극을 받아서 진전된 상태를 말함.
위 험 성	특정한 위험 사건이 발생할 가능성과 결과의 조합	위험이 어떤 자극을 받아서 진전될 가능성(발생빈도)과 진전되었을 때 나타날 수 있는 결과(피해크기)를 결합시켜서 위험의 크기나 정도를 나타낸 것을 말함.
위험성 평가	위험성의 크기를 추정하고, 그 위험성이 허용가능한지를 결정하는 전체 프로세스	위험성을 파악하여 그 위험성이 안전 범주 내에 있는지를 판단하는 전반적인 과정을 말함.

주) OHSAS 18001:1999 /K-OHSMS 18001:2001을 근거로 필자 작성하였음.

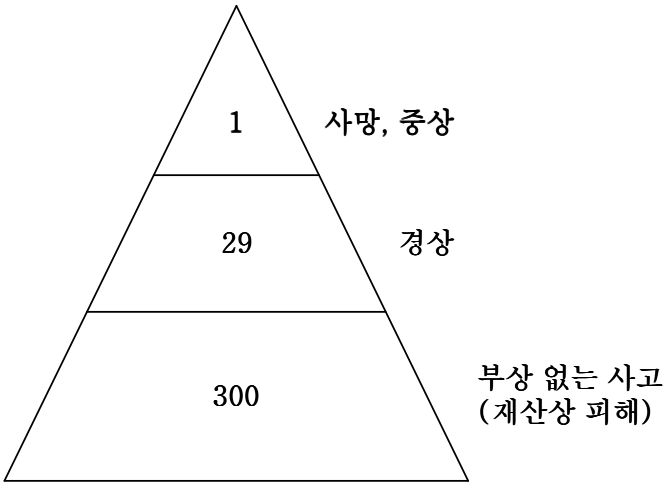
제3절 사고와 손실의 인과 관계에 대한 이론적 전개

제2절에서 안전은 수용할 수 없는 피해의 위험성으로부터 자유로운 것이라고 정의하였으며, 위험성은 특정한 위험 사건이 발생할 가능성과 결과의 조합이라고 하였다. 그리고 사건은 사고를 발생시키거나 사고로 이어질 가능성이 있는 사상이라고 하였으며, 사고는 사망, 건강상 장해, 부상, 손해 기타 손실을 발생시키는 의도하지 않은 사상이라고 정의 하였다.

이를 종합하면 손실은 사고의 결과로서 나타나는 것이며 의도하지 않은 피해나 손상을 발생시킨다. 안전을 확보한다는 것은 손실을 없애거나 수용할 수 있는 범위내로 줄이는 것이며 이는 사고를 관리함으로써 가능해질 수 있다. 그러므로 사고의 발전 단계와 손실과의 인과 관계를 규명해봄으로써 안전을 확보하기 위한 구체적인 접근 방법을 찾을 수 있을 것이다.

사망이나 중상을 야기하는 중대한 사고가 어느 한 순간에 일어난다고 생각할 수 있지만 여러 조사에 의하면 이런 심각한 사고는 어느 한 순간에 발생하는 것이 아니고 일정한 진행 과정을 거쳐서 나타나는 것을 볼 수 있다. 하인리히(H. W. Heinrich)는 이를 1:29:300의 논리로 설명하고 있다.[35] 즉, 1건의 사망 또는 중상 사고가 발생하기까지는 29건의 경미한 부상 사고가 있었으며, 29건의 경미한 부상 사고가 발생하기까지는 300건의 부상이 없는 사고가 발생한다는 것이다. 다시 말하면 1건의 심각한 사고는 300건의 부상이 없는 사고로부터 진전되는 것이다. 이를 그림으로 나타내면 <그림 3-1>과 같다.

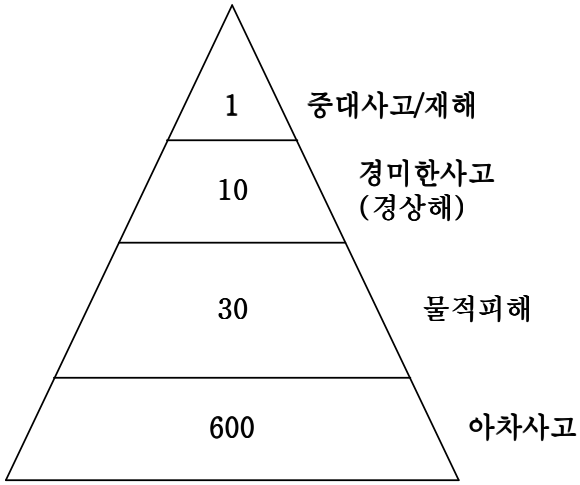
<그림 3-1> 하인리히의 사고 비율 연구



35) 김영호, 고재욱, 김동환, 임동호, 윤석준 편저, 「안전·보건 경영 실무」, 대영사, 2000, pp.5-6 (원저. Frank E. Bird. Jr., George L., Germain, 「Practical Loss Control Leadership」, Det Norske Veritas(U.S.A), Inc. 1996).

하인리히의 연구는 한 사람과 관련된 같은 종류의 사고에 대한 분석이었다. 1969년에 버드(Frank E. Bird Jr.)는 전체 노동자를 대상으로 실제 보고된 사고 사이에 어떤 결과가 있는지에 대하여 연구하고 1:10:30:600의 논리로 설명하고 있다.[36] 즉, 1건의 중대한 사고에는 10건의 경상 사고가 있었으며, 또 30건의 재산피해 사고가 있었고 600건의 사고가 날 뻔했던 사건이 있었다는 것이다.[37] 이를 그림으로 나타내면 <그림 3-2>와 같다.

<그림 3-2> 버드의 사고 비율 연구



이런 두 가지 연구 결과로 볼 때 심각한 사고는 갑작스럽게 바로 발생하는 것이 아니고 사고로 이어질 가능성이 있는 사상(事象)인 사건 단계에서 점점 진전되어 중대한 사고가 된다. 그러므로 사건이 사고로 진전되는 것을 막으면 궁극적으로 손실의 발생을 예방할 수 있는 것이다[38].

앞에서 손실은 사고의 결과로써 나타나는 것이고 사고는 사건이 진전되어 발생하는 현상이라고 하였다. 그리고 사건이 사고로 진전되는 것을 막으면 손실의 발생을 방지할 수 있다고 하였다. 그러면 여기서 사건이 발생하는 부분에 대해서 고찰할 필요가 있다.

손실이 사건으로부터 진전되어 나타나듯이 사건도 일정한 진전단계를 거쳐서 발생한다. 사건과 가장 가까운 시점에 있는 것이 직접적 원인이다. 직접적 원인은 사건이 일어나기 바로 전에 발생하는 것이며 대부분 감지가 될 수 있는

36) 김영호 외 4인, 전게서, pp. 6-7.

37) Frank E. Bird Jr.는 총 297개 협력업체에서 보고 된 1,753,498건의 사고에 대한 분석을 하였다. 이 회사들은 21개의 다양한 업종이었으며, 이 연구는 1,750,000명의 종업원이 30억 시간에 걸쳐 근무한 시간을 대상으로 분석하였다.

38) 김영호 외 4인, 전게서. pp. 7.

것 들이다. 직접적 원인은 기준이하의 행동이나 관습 그리고 기준이하의 상황으로 구분하여 이해하는 것이 필요하다(<표 3-2> 참조).

<표 3-2> 사건의 직접적 원인

기준 이하 행동 혹은 관습	기준 이하 상황
1. 인가 없이 장비 작동 2. 경고 행위를 않음 3. 안전을 확보하지 않음 4. 부적절한 속도로 장비 작동 5. 안전장비를 없애거나 작동하지 않게 함 6. 결함 있는 장비의 사용 7. 부적절한 방법으로 장비 사용 8. 개인 보호 장비를 적절히 착용하지 않음 9. 부적절한 하역 작업 10. 부적절한 물건 배치 11. 부적절한 양중기 작업 12. 부적절한 작업 위치 13. 작동중인 장비의 수리 14. 소란 15. 알코올 또는 약물 복용 중 작업 16. 작업절차를 제대로 이행하지 않음	1. 부적절한 방호구나 보호벽 2. 부적합한 보호 장비 3. 결함 있는 도구, 장비나 재료 4. 혼잡, 내지는 행동이 제약되는 상황 5. 부적합한 경고 시스템 6. 화재와 폭발위험 7. 부적절한 보관, 무질서한 작업장소 8. 위험한 환경조건: 가스, 먼지, 연기, 증기 등 9. 소음 노출 10. 방사능 노출 11. 고/저온 노출 12. 부적절한 조명 13. 부적절한 환기

자료 : 김영호 외 4인, 전게서, pp. 13-14.

모든 직접적 원인이 반드시 사건으로 진전되는 것은 아니나 모든 직접적 원인은 사건이 발생할 수 있는 징후라고는 볼 수 있다. 이런 징후 뒤에는 또 다른 원인이 있으므로 직접적 원인을 이해하려면 다음과 같은 질문을 가져야 한다.

“왜 그런 기준이하의 행동 또는 관습이 발생했는가?”

“왜 그런 기준이하의 상황이 존재했는가?”

이런 질문에 대한 해답을 찾으면 직접적 원인 뒤에 숨겨진 근본 원인을 규명

할 수 있다. 근본 원인을 찾으면 사람들이 기준이하의 행동이나 관습을 하는 이유 또는 기준이하의 상황이 존재하는 이유를 설명할 수 있다. 직접적 원인이 쉽게 감지될 수 있는 것에 비해 이 근본 원인은 쉽게 감지되지 않으며 정밀한 조사가 있어야 확인할 수 있는 것이 보통이다. 직접 원인이 기준이하의 행동이나 관습 그리고 기준이하의 상황과 같이 2부분으로 나누는 것과 같이 근본 원인도 인적 요인과 업무/시스템적 요인으로 구분하는 것이 바람직하다(<표 3-3> 참조).

<표 3-3> 사건의 근본원인

인적 요인	업무/시스템적 요인
1. 부적절한 능력 · 육체적/생리학적 · 정신적/심리학적 2. 지식부족 3. 기술부족 4. 스트레스 · 육체적 스트레스 · 정신적 스트레스 5. 부적절한 동기부여	1. 부적절한 지도력과 관리감독 2. 부적절한 기술 공학 3. 부적절한 구매 4. 부적절한 유지 관리 5. 부적절한 도구, 장비, 원자재 6. 부적절한 작업기준 7. 마모와 파손 8. 남용 혹은 요용

자료 : 김영호 외 4인, 전게서, pp. 24.

근본 원인은 직접적 원인인 기준이하의 행동/관습 및 기준이하의 상황이 발생하게 되는 근원이다. 그러나 이것이 사고와 손실 인과 관계의 발단이 되는 것은 아니다. 근본 원인이 존재하게 되는 이유는 관리 부재에 있다.

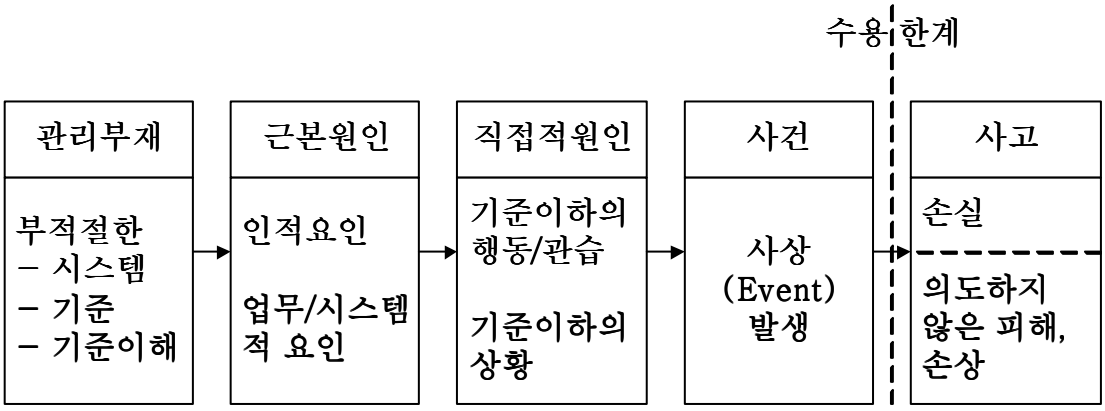
관리란 조직의 기준을 정확히 이해하고, 기준을 맞추기 위한 계획을 수립하여야 하며, 수립된 계획에 따라 적절한 이행을 하여야 하며, 이행된 결과를 평가하고, 평가 결과에 따른 적절한 조치를 시행하는 것이다. 데밍(Deming)은 이를 네 가지 기능, 계획(Plan), 이행(Do), 점검(Check), 그리고 조치(Action) 기능으로 규정하였다.[39] 이들 네 가지 기능이 유기적으로 잘 운용이 될 때는 사고를 유발하는 요소가 발생하지 않지만 그렇지 않은 경우는 사고 인과 관계가 시작되며 손실을 일으키는 요소가 끊임없이 발생하게 되고 이에 대한 적절한

39) 안영진, 「21세기 기업경쟁력 강화를 위한 TQM:품질경영」, 박영사, 2000, pp. 439.

대응 조치가 이루어지지 않으면 손실에 이르게 된다. 관리 부재에서 나타나는 일반적인 세 가지 부분은 부적절한 시스템, 부적절한 기준, 기준을 이행하지 않는 것이다.

위에서 설명한 내용을 종합하여 사고와 손실의 인과 관계를 정리하면 다음과 같다. 관리 부재로부터 근본 원인이 발생하며, 근본 원인이 직접적 원인을 제공하고, 직접적 원인으로부터 사건이 생기며, 사건의 일부는 사고로 진전되고 사고는 손실을 초래하게 된다(<그림 3-3> 참조).

<그림 3-3> 사고와 손실의 인과 관계 모델



자료 : 김영호 외 4인, 전게서, pp. 9.

이 인과 관계를 통해서 알 수 있는 것은 손실을 초래하는 사고는 많은 단계를 거쳐야 하고 또한 많은 요소들이 복합적으로 작용하고 있다는 것이다. 그러므로 사고에 이르는 단계 및 사고의 원인을 파악하여 적절히 관리한다면 사고의 발생을 방지할 수 있고 그 결과 손실을 초래하지 않는다는 것이다.

제4절 위험성 평가

1. 위험성 평가의 이론적 전개

사고와 손실의 인과 관계에서 사고를 막기 위해서는 사고의 원인이 되는 직접적 원인, 근본 원인 및 관리 부재에 숨어 있는 위험 요소들을 찾아내서 제거하거나 적절히 관리하면 사고로 진전되지 않는다는 것을 알 수 있었다.

위험성 평가는 숨어있는 위험 요소를 파악하고 사고의 종류, 사고가 발생할 수 있는 확률과 피해의 크기를 예측하여 손실의 정도가 허용 가능한지를 확인

하는 전체 과정이다. 이것을 앞에서 위험성의 크기를 추정하고, 그 위험성이 허용가능한지를 결정하는 전체 프로세스라고 정의하였다.

위험성을 평가하기 위해서는 먼저 위험성의 크기를 추정하는 과정이 있어야 한다. 위험성은 특정한 위험 사건이 발생할 가능성과 결과의 조합으로 얻어질 수 있다. 이는 다음과 같이 표현할 수 있다.

위험성(Risk)을 R, 발생 가능성(Probability)을 P, 결과(Consequence)를 C라고 하면

R = P * C 이다.[40]

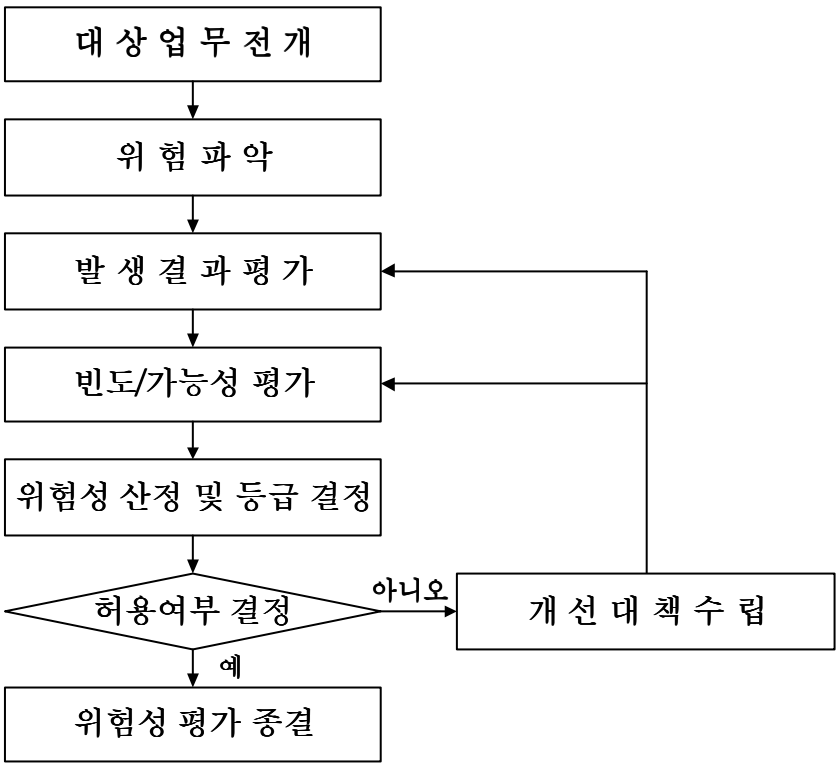
위험성을 구하려면 사건의 발생 가능성과 결과를 알아야 된다. 사건의 발생 가능성과 결과는 사건이 일어난다는 것을 전제로 한 것이므로 사건이 일어나기 위해서는 내재되어 있는 위험이 진전되어야 한다. 그러므로 위험의 존재를 인식하고 그것의 특성을 규정하는 위험 파악 과정을 통해서 위험을 충분히 식별하여야 하는 것이 선행되어야 한다. 그리고 이 위험 파악은 수행하고 있는 업무를 충분히 전개시켜야 그 업무 속에 내재되어 있는 모든 위험을 파악할 수 있다.

결국 위험성을 평가한다는 것은 특정한 시스템이나 작업이 수행되고 있는 현상을 충분히 전개시키고, 그 속에 잠재되어 있는 위험 요소들을 찾아내고 이것들로부터 발생 가능한 사고나 손실의 특성을 파악하고, 나아가 발생빈도와 결과까지 예측하여 위험성의 크기를 추정하고, 그 크기가 수용가능한지를 판단하는 과정까지이다. 이것이 일반적인 위험성 평가 프로세스이다.

그러나 잠재된 위험으로부터 안전을 확보하고자 한다면 평가 결과 수용할 수 없는 위험성이 식별된 경우에 그 위험성을 허용 가능한 범위 내의 위험성으로 만들기 위한 방법을 찾는 과정이 필수적으로 시행되어야 한다. 그래서 본 연구에서는 위험성 평가의 과정을 수용할 수 없는 위험성이 식별된 경우에 허용 가능한 범위 내의 위험성으로 만들기 위한 대책을 찾는 과정까지로 확대하여 적용하고자 하며 위험성 평가의 전체적인 과정을 표시하면 다음과 같다 (<그림 3-4> 참조).

40) 한국산업안전공단(KOSHA)의 안전보건 경영시스템 구축에 관한 지침(KOSHA Code G-04-2003, 공표일 2003. 12. 31.). 부록 2.

<그림 3-4> 위험성 평가 체계도



2. 위험성 평가 방법의 종류

위험성 평가를 하는 방법은 크게 두 가지로 분류할 수 있다. 위험을 식별하고 발생 가능성 및 결과를 얻는 방법에서 정확한 데이터를 바탕으로 확률적으로 평가하는 정량적 평가방법인 Hazard Assessment Methods와 정확한 데이터나 확률 값은 구하지 못하지만 직접적인 경험과 간접적인 경험을 토대로 어떤 위험이 존재하는지를 찾아내는 정성적 분석방법인 Hazard Identification Methods이다. 정량적 평가방법과 정성적 분석방법의 종류는 다음과 같다[41] (<표 3-4> 참조).

위험성 평가 방법은 평가 목적, 평가 대상 또는 평가 시기 등에 따라 달라질 수 있으나 위험을 식별하고, 위험성을 평가하여 안전을 확보하기 위한 조치를 취하는 데는 공통적인 특징을 가지고 있다.

41) 주종대, 조지훈, 「위험과 운전분석(HAZOP)」, 한국산업안전공단, 전문교육자료, 2001, pp. 33.

<표 3-4> 위험성 평가 방법의 종류

정성적 평가방법 (Hazard Identification Methods)	정량적 분석방법 (Hazard Assessment Methods)
1. 공정/시스템 체크리스트 (Process/System Checklist) 2. 안전성 검토(Safety Review) 3. 상대위험순위(Relative Ranking) 4. 예비위험분석(PHA: Preliminary Hazard Analysis) 5. 사고예상 질문 분석(What-if)) 6. 위험과 운전분석(HAZOP) 7. 이상 위험도분석(FMECA: Failure Modes, Effects, and Criticality Analysis)) 7. 작업자실수 분석(HEA: Human Error Analysis)	1. 결함수 분석(FTA: Fault Tree Analysis) 2. 사건수 분석(ETA: Event Tree Analysis) 3. 원인-결과 분석(CCA: Cause-Consequence Analysis)

자료 : 주종대, 조지훈, 전게서, 2001, pp. 33.

정확한 데이터를 구할 수 있는 경우에는 정량적인 평가가 가능하여 위험성 평가 결과치도 정확한 것을 얻을 수 있지만 정확한 데이터가 없거나 구하는데 어렵고 장시간이 소요된다면 위험성 평가 자체가 진행될 수 없다. 그러므로 정확한 데이터를 구할 수 없는 경우에는 직간접적인 경험이 바탕이 되는 정성적 평가방법으로 위험성 평가를 진행한다. 정성적 평가방법과 정량적 분석방법의 차이는 다음과 같다(<표 3-5> 참조).

<표 3-5> 위험성 평가의 정성적 평가방법과 정량적 분석방법의 장·단점

	장 점	단 점
정성적 평가방법	1. 비교적 쉽고 빠른 결과 도출 2. 비전문가도 시행 가능 3. 평가하는 시간과 경비 절감	1. 주관적 평가에 치우칠 우려가 있음
정량적 분석방법	1. 객관적, 정량화된 결과 도출	1. 평가하는 시간과 경비가 과다 2. 전문가 필요 3. 통계 데이터 확보 어려움 및 신뢰성 불확실

주) 주종대, 조지훈의 전게서, 2001, pp. 41부터 82까지 참조하여 필자 정리하였음.

제5절 위험성 평가 시행 방법

<그림 3-4>에 전개된 위험성 평가 과정을 기준으로 각 단계별로 수행하여야 할 방법은 다음과 같다.

1. 운영 중인 시스템이나 수행 중인 작업에 대한 전개

위험성 평가를 하기 위한 첫 번째 단계는 위험성 평가를 하고자 하는 대상을 정확히 파악하는 것이다. 대상을 정확히 파악하는 것은 먼저 어떤 부분에 대해서 위험성을 평가할 것인지 구체적으로 결정하여야 한다. 그리고 결정된 부분에 대한 설명이 상세하게 전개되어야 한다. 즉 현재 수행하고 있는 업무의 목적, 업무 수행 방법, 적용되고 있는 강제 규정이나 기준, 작성된 업무 표준, 사용하고 있는 장비, 설비, 기기 및 소프트웨어 등이 모두 파악되어야 한다. 그리고 또 하나 누락시키지 않고 파악해야 할 사항은 현재 시행 중에 있는 안전장치에 대한 것이다. 이 안전장치에 관한 것은 후속 단계인 발생 가능성과 밀접한 관계가 있으므로 이 단계에서 누락되지 않게 파악하여야 한다. 이 과정이 위험성 평가에서 가장 중요한 과정이라고는 할 수 없지만 이것을 생략하거나 충실히 수행하지 않을 경우에는 다음 단계인 위험 파악 단계에서 찾고자 하는 위험을 충분히 식별하지 못하게 된다.

2. 위험 파악

운영 중인 시스템이나 수행 중인 작업에 대한 전개가 충분히 완료되고 나면 다음 단계는 이 속에 내재되어 있는 위험을 찾아내는 것이다.

위험 파악 단계에서는 시스템이나 작업 수행 과정에 숨어있는 위험 요소를 모두 찾아내야 하며 그 위험 요소들이 가지고 있는 특성을 정확히 규명해야 한다. 그리고 필요하다면 그 특성들은 분류를 하는 것이 필요하다.

위험 파악은 <그림 3-4>에서 보는 것과 같이 위험성 평가 절차의 기초가 된다. 그러므로 효과적인 위험성 평가가 진행되려면 위험 파악이 철저하게 수행되어야 한다. 만약 위험 파악이 생략되거나 정확하게 실시하지 않는다면 이것을 기반으로 한 후속단계에서의 결정은 무의미하게 될 것이다. 그러므로 이 단계를 위험성 평가 단계에서 가장 중요한 단계로 인식하는 것이 필요하다.

위험 파악을 위해서는 많은 분야의 사람들이 참석하는 것이 필요하다. 일부 몇 사람만 참여하여 위험 파악을 수행하면 제한된 시각의 위험만 식별이 될 수

있다. 그러므로 내재되어 있는 위험을 누락시키지 않고 식별하기 위해서는 위험성 평가 대상과 관계되는 모든 분야를 대표하는 사람들이 참석하여 위험 파악을 진행하여야 한다.

위험 파악을 할 때는 두 가지 기본적인 접근 방법이 있다. 먼저 이미 축적된 경험과 근거 규정을 활용하는 것과, 경험이 축적되어 있지 않은 경우 적용하는 예측 위험 요소 파악 방법이다.[42)]

파악된 위험에 대해서는 그 위험이 발생할 수 있는 원인들을 면밀히 검토하여 식별한다. 한 가지 이상의 원인이 있는 경우에는 해당되는 모든 원인을 식별하여야 한다. 이 원인은 향후 개선 대책을 수립하는데 직접적인 영향을 미치므로 누락되지 않고 식별하는 것이 필요하다.

3. 발생 결과 평가

발생 결과 평가에서는 앞 단계에서 파악된 위험이 사고로 진전되었을 경우에 나타나는 결과에 대하여 평가하는 것이다. 예상되는 결과도 원인과 마찬가지로 한 가지 이상의 결과가 나올 수 있다. 이 경우 예상되는 모든 결과를 파악하여야 한다.

4. 빈도/가능성 평가

빈도/가능성 평가에서는 파악된 위험이 사고로 진전될 수 있는 빈도나 가능성을 평가한다. 해당 업무를 수행 중에 얼마나 자주 위험을 맞이하게 되는지 그리고 위험을 맞이했을 경우에 사고로 진전될 수 있는지를 평가하여야 한다.

빈도/가능성을 평가할 때는 현재 수행 중에 있는 업무 절차, 적용하고 있는 기준 그리고 현재 적용되고 있는 안전조치를 고려하여 판단하여야 한다. 즉 동일한 업무라고 하더라도 안전 조치가 불충분한 경우에는 가능성은 높게 나올 것이며 현재 충분한 안전 조치가 적용되고 있다면 가능성은 그만큼 줄어들 것이다.

5. 위험성 산정 및 등급 결정

예상되는 결과와 빈도/가능성을 근거로 위험성의 크기를 확정하고 등급을 산정한다. 위험성 등급 결정은 위험성 분석 과정을 단순화하는데 가장 효과적

42) 주종대, 조지훈, 전게서, pp. 34-37.

이며 위험에 따른 대응을 하기위한 우선순위를 결정하도록 한다. 위험성 등급 결정은 간단하지만 체계적인 기법으로서 위험성의 허용가능여부의 결정 및 위험성을 낮추기 위한 투자의 우선순위를 결정하는데 많은 도움을 준다.

위험성의 크기를 확정하고 등급을 산정하는 방법은 행렬 매트릭스를 사용하여 구하는 것이다. 발생 결과 평가에서 구한 것과 빈도/가능성 평가에서 구한 것을 각 각 등급으로 분류한 후 이 두 가지 등급을 가지고 행렬 매트릭스를 구성한다.

먼저 피해의 심각성을 나타내는 발생 결과 평가의 등급을 다음과 같이 분류한다(<표 3-6> 참조).

<표 3-6> 발생 결과(심각성) 구분

등 급	내 용
3(높음)	사망, 중상 발생, 재산 피해 10억 원 이상 작업중지 10일 이상
2(중간)	경상 발생, 재산 피해 1～10억원 작업중지 1～10일
1(낮음)	부상자 없음, 재산 피해 1억원 미만 작업중지 1일 미만

다음으로 위험이 사고로 진전될 정도를 나타내는 빈도/가능성을 나타내는 등급을 다음과 같이 분류한다(<표 3-7> 참조).

<표 3-7> 빈도/가능성 구분

등 급	내 용
3(높음)	설비 수명기간에 한 번 이상 발생 즉시 발생할 것 같음
2(중간)	설비 수명기간에 가능성 있음 얼마 후 발생할 것 같음
1(낮음)	설비 수명기간에 가능성 희박함 한참 뒤 일어날 수도 있음

위험성의 크기를 확정하고 등급을 산정하는 행렬 매트릭스는 심각성과 빈도/가능성으로 구성한다(<표 3-8> 참조).

<표 3-8> 위험성 등급 구분

심각성 / 가능성	3(높음)	2(중간)	1(낮음)
3(높음)	5	4	3
2(중간)	4	3	2
1(낮음)	3	2	1

각 위험성 등급은 다음과 같은 의미로 정의한다.

(1) 위험성 등급 5 : 매우 중대함, 수용 불가
(2) 위험성 등급 4 : 심각함, 중대
(3) 위험성 등급 3 : 보통, 보통
(4) 위험성 등급 2 : 경미함, 수용가능
(5) 위험성 등급 1 : 무시, 작음

위험성 등급을 산정한 결과 등급이 5 또는 4가 나오는 경우는 위험성 등급을 낮추기 위한 대책이 반드시 시행되어야 하는 등급이다.

위험성 등급이 3인 경우에는 위험성 등급을 낮추기 위한 대책이 필요한지 검토하고 필요한 경우에 한하여 추가 대책을 시행하는 것이 요구된다.

위험성 등급이 2 또는 1인 경우에는 별도의 추가 대책이 필요 없는 경우이다.

6. 개선대책 수립

위험성 등급이 5 또는 4로 결정된 사항에 대해서는 반드시 위험성 등급을 3 이하로 낮출 수 있는 개선대책을 수립하여야 한다. 개선대책은 현재 적용되고 있는 안전조치 이외의 조치가 적용되어야 하므로 개선대책을 파악할 때는 현재의 안전조치사항은 고려 대상에서 제외하여야 한다.

개선대책을 수립할 때는 위험을 발생시키는 원인을 근본적으로 제거하는 방법을 가장 먼저 고려하여야 하며, 원인을 근본적으로 제거하는 것이 불가능 할 경우에는 위험이 사고로 진전되지 않도록 적절히 관리하기 위한 방법을 다음

으로 고려하여야 하고, 위험이 진전되어 사고가 발생하였을 때 피해를 최소화할 수 있는 방법을 마지막으로 고려하여야 한다.

또한 개선대책을 수립할 때는 심각성에 해당되는 발생 결과의 등급을 낮추는 것보다 빈도/가능성의 등급을 낮추는 방향으로 대책을 수립하는 것이 바람직하다.

일반적으로 발생 결과 등급을 낮추기 위해서는 많은 비용과 장기간의 기간이 소요되므로 개선 대책이 실천 불가능하거나 상당한 시일이 요구된다. 만일 발생 결과의 등급만 낮추는 개선 대책을 수립한 경우에는 장기간 아무런 조치도 시행되지 않을 수 있다. 그러면 사고가 발생할 확률은 높아지기 마련이며 피해도 커질 수 있다. 빈도/가능성의 등급을 낮추기 위한 대책은 상대적으로 발생 결과를 낮추기 위한 대책보다 시행에 들어가기가 쉬운 것들이다. 예를 들어 업무 절차의 변경, 작업자에 대한 교육 시행 등과 같이 비교적 단기간에 계획을 세워서 진행이 가능한 것들이다. 그러므로 빈도/가능성의 등급을 낮출 수 있는 대책을 먼저 시행하고 장기적으로는 발생 결과 등급을 낮출 수 있는 대책을 병행하는 것이 바람직하다.

다음으로 개선대책을 수립할 때 고려하여야 하는 것을 비용 효과 분석을 하는 것이다. 투입한 비용에 비해서 얻을 수 있는 효과가 만지 않은 경우 또는 과도한 비용이 투자가 되는 경우에는 개선 대책으로서 부적절할 수 있다. 이런 경우에는 다른 대책을 수립할 필요가 있다.

그리고 개선대책이 기술적인 향상을 필요로 하는 경우에는 현재 기술로서 달성 가능한 정도인지 아닌지를 판단하여야 한다. 만약 달성 가능한 정도가 아닌 경우에는 기술 개발에 투자되는 비용에 대한 비용 효과 분석을 통해서 적절한 개선대책인지를 판단하여야 한다.

7. 개선대책에 대한 위험성 재평가

적용 가능한 개선대책을 수립한 경우에는 개선대책을 실행에 옮기기 전에 이 개선대책이 실제적으로 위험성 등급을 낮추는지를 확인하여야 한다. 이를 확인하기 위해서는 발생 결과 평가부터 다시 시작하여 위험성 등급을 확인하여야 한다. 재평가 결과 위험성 등급이 수용할 수 있는 범위내로 낮추어진 경우에는 이 개선대책을 채택할 수 있지만 그렇지 못한 경우에는 이 개선대책은 적절한 개선대책으로 볼 수 없으므로 다른 개선대책을 강구하여야 한다.

제6절 ISPS Code에서 요구하는 항만시설 보안평가

항만시설 보안평가는 항만시설의 보안시스템인 항만시설 보안계획서를 수립하기 위하여 필요한 부분이라고 ISPS Code에서는 밝히고 있다. 그리고 항만시설 보안평가에 적용되는 요건을 규정하고 있다. 그러므로 항만시설 보안평가를 시행하기 위한 적절한 보안평가 방법론을 수립하기 위해서는 ISPS Code에서 요구하고 있는 항만시설 보안평가 요건을 정확히 분석하는 것이 요구된다.

1. ISPS Code에 규정된 항만시설 보안평가 요건

항만시설 보안평가와 관련하여 ISPS Code에 규정된 사항들 중에서 항만시설 보안평가에 대한 당사국 정부의 책임 사항 및 행정적인 조치를 요구하는 사항들을 제외하고 실제적인 항만시설 보안평가를 시행하는 요건들을 요약하면 다음과 같다.

1) 항만시설보안평가는 최소 다음 요소들을 포함하여야 한다(A편/15.5).
   (1) 중요하게 보호되어야 하는 주요자산 및 기반시설의 식별 및 평가
   (2) 보안조치의 수립 및 이들의 우선순위를 정하기 위하여 자산 및 기반시설에 대한 가능한 위협과 발생 가능성을 식별
   (3) 취약성을 감소시킴에 있어 대응조치 및 절차변경 그리고 유효성의 수준을 식별, 선택 및 우선순위를 결정
   (4) 기반시설, 정책 및 절차에 있어서 인적요소를 포함한 약점을 식별

2) 항만시설 보안평가는 공격의 대상이 될 수 있거나 이러한 가능성이 더 높은 부분을 결정하기 위한 항만시설 운영의 모든 측면에서의 근본적인 위험성 분석이다. 보안위험성은 표적에 노출될 취약성 및 공격의 결과가 결부된 공격위협의 함수 작용이다(B편/1.17).

3) 항만시설 보안평가는 다음의 구성요소들을 반드시 포함하여야 한다(B편/1.17).
   (1) 항만시설 및 기반시설에 대해 인지된 위협은 반드시 결정되어 질 것
   (2) 잠재적 취약성이 식별되어 질 것
   (3) 사고의 결과가 추산되어 질 것

4) 중요하게 보호되어야 하는 주요자산 및 기반시설의 식별 및 평가

주요자산 및 기반시설의 식별 및 평가는 이를 통하여 항만시설의 기능에 주요한 구조 및 설비의 상대적인 중요성을 수립할 수 있게 하는 프로세스이다. 이 프로세스는 보안사건으로부터 보호하기에 더 중요한 자산 및 설비에 대한 경감전략에 집중할 수 있는 근간을 마련한다. 이 프로세스는 잠재적인 인명손실, 항만의 경제적 중요성, 상징적 가치, 정부시설의 유두 등을 고려하여야 한다(B편/15.5).

주요자산 및 기반시설의 식별 및 평가는 보호 대상이 상대적 중요성에 대하여 우선순위를 정하는데 사용되어져야 한다. 우선적으로 고려할 점은 사망 및 부상의 회피에 있어야 한다. 또한 항만의 시설, 구조물 또는 설비들이 그러한 자산이 없더라도 정상작동이 가능한지 그리고 정상기능을 위한 신속한 재건축 등이 가능한지의 범위 등을 고려하는 것이 중요하다(B편/15.6).

자산 및 기반시설은 중요하게 보호되어야 하며 다음 사항들을 포함한다(B편/15.7).

(1) 통행로, 출입구, 접근로, 묘박지, 선박 조종 지역, 접안 지역
(2) 화물 설비, 터미널, 화물 보관구역, 화물 취급 장비
(3) 전기 배선 시스템, 무선 및 원격통신시스템, 컴퓨터 시스템, 네트워크
(4) 항내 선박 통항 관제 시스템 및 항로표지
(5) 발전소, 화물 이송 파이프, 수도 시설
(6) 교량, 철도, 도록
(7) 항내 서비스 선박(도선선, 예인선, 부선 등)
(8) 보안 및 감시 장비와 시스템
(9) 항만시설에 인접한 수역

자산 및 기반시설에 대한 명확한 식별은 항만시설의 보안 요건의 평가, 예방조치의 우선순위 설정 그리고 항만시설의 더 나은 보호를 위한 자원의 할당과 관련된 결정 등을 위하여 필수적이다(B편/15.8).

5) 보안 조치의 우선순위를 정하기 위한 자산 및 기반시설에 대한 예상 위협 및 발생가능성의 식별

해당 자산 또는 장소에 대한 취약성을 평가하고 계획 및 자원 할당이 가능하도록 보안요건의 우선순위를 수립하기 위하여 자산과 기반시설의 보안에 위협을 줄 수 있는 행위 및 그러한 행위를 실행할 수 있도록 하는 수단들이 식별되어야 한다. 각각의 잠재적인 행위 및 그 수단들에 대한

식별 및 평가는 정부기관에 의한 위협평가를 포함한 다양한 요소들에 기초하여야 한다(B편/15.9).

항만시설 보안평가는 보안조치가 개발되어야 하는 위험성 수준에 대한 전반적 평가를 산출하여야 한다(B편/15.10).

항만시설 보안평가는 다음과 같은 형식의 보안사건 들을 포함하여 모든 가능한 위협에 대하여 고려하여야 한다(B편/15.11).

(1) 폭발장치, 방화, 파괴행위와 같은 항만시설 또는 선박의 손상 및 파괴
(2) 선박 또는 선박에 승선한 인원의 납치 또는 강탈
(3) 화물, 선박의 주요 설비 및 시스템 또는 선용품에 대한 조작
(4) 밀항자를 포함한 불법 출입 및 이용
(5) 대량살상무기를 포함한 무기 및 장비의 밀수
(6) 보안사건을 일으킬 수 있는 사람들이나 그들의 장비를 이송하기 위한 선박의 사용
(7) 손상 또는 파괴수단 또는 무기로서 선박자체의 사용
(8) 항만 입구, 갑문, 접근로 등의 봉쇄 등
(9) 핵, 생화학적 공격

6) 취약성을 감소시키기 위한 대응방안, 절차의 변경 및 유효성 수준에 대한 식별, 선별 및 우순순위의 결정

대응방안을 식별하고 우선순위를 결정하는 것은 발생 가능한 위협에 대하여 항만시설 또는 선박/항만인터페이스의 취약성을 줄이기 위하여 가장 효과적인 보안조치가 도입되도록 하여야 한다(B편/15.13).

보안조치는 공격가능성의 감소여부 등과 같은 요소를 토대로 선택되어야 하며 다음을 포함하는 정보를 사용하여 평가되어져야 한다(B편/15.14).

(1) 보안검사, 점검 및 심사
(2) 항만설비 소유자 및 운영자 또는 타당한 경우 인근 구조물의 소유자/운영자와의 협의
(3) 보안사건에 대한 역사적 정보
(4) 항만시설 내에서의 운영

7) 취약성의 식별

물리적인 구조, 개인 보호 시스템, 프로세스 또는 보안사건이 일어날 수 있는 어떤 분야에 대한 취약성 식별은 그러한 취약성을 제거하거나 완화시키는 조치를 수립하는데 적용될 수 있다(B편/15.15).

2. 항만시설 보안평가의 목적 및 의의

ISPS Code에서 요구하는 항만시설 보안평가에 대한 요건을 분석하면 다음과 같이 항만시설 보안평가의 목적 및 의의를 찾을 수 있다.

1) 목적

항만시설 보안평가는 항만시설 보안계획서를 개발하기 위하여 또는 개발되어 시행되고 있는 항만시설 보안계획서를 최신화 시키기 위하여 시행한다. 항만시설 보안계획서는 항만시설의 보안시스템을 나타내고 있는 것으로서 항만시설의 보안조직, 보안임무 및 각 보안등급별로 항만시설에의 접근, 항만시설 내의 제한구역, 화물의 취급, 선용품의 인도, 미휴대 수화물의 취급, 항만시설 보안 모니터링 등에 대하여 항만시설에서 시행해야 하는 보안조치 및 보안절차를 표함하고 있다

이러한 항만시설 보안계획서는 항만시설 보안평가를 근거로 개발되고 유지되어야 한다.[43] 그러므로 항만시설 보안평가는 항만시설 보안계획서를 개발하고 적절히 유지하기 위한 기초적인 자료를 제공하는데 목적이 있다.

2) 의의

항만시설 보안계획서를 개발하고 최신화시켜서 유지하기 위한 기초적인 자료를 제공하는 것이 목적인 항만시설 보안평가는 항만시설 운영의 모든 분야에 대한 근본적인 보안위험성 분석을 하는데 그 의의가 있다. 그리고 이런 보안위험성 분석을 통하여 보안조치가 개발되어야 하는 위험성 수준에 대한 전반적인 결정을 구할 수 있다.

다음으로 위험성 수준을 감소시키기 위한 대응 조치 방법을 모색하는 것이 항만시설 보안평가의 또 다른 의의라고 할 수 있다.

제7절 항만시설 보안평가

1. 항만시설 보안평가의 구성요소

항만시설들이 항만시설 보안계획서를 수립하기 위하여 필수적으로 수행하여야 하는 항만시설 보안평가를 통하여 확인하고 결과를 도출하여야 할 사항들

43) ISPS Code Part A. / 16.1.

에 대하여 ISPS Code에 규정된 요건을 분석하면 다음과 같은 항만시설 보안평가 요소들을 확인할 수 있다.

1) 보호해야 될 주요자산 및 기반시설 식별
2) 식별된 주요자산 및 기반시설에 대한 우선순위 평가
3) 발생 가능한 보안위협 식별
4) 식별된 보안위협에 대한 발생가능성 식별
5) 사고의 결과 추산
6) 취약성을 감소시키는 대응조치 식별
7) 대응조치에 대한 우선순위 식별
8) 보안과 관련한 항만시설의 취약점 식별

즉 항만시설은 항만시설 보안평가를 통하여 위에 제시된 구성요소에 대한 결과를 도출하고 이들을 항만시설 보안계획서에 반영하여야 한다.

2. 항만시설 보안평가와 연관된 개념들에 대한 정의

항만시설 보안평가에 대한 방법론을 구하기 위해서는 먼저 항만시설 보안평가와 관련된 부분들에 대한 개념 정의가 필요할 것이다.

1) 보안

보안은 다음과 같이 정의될 수 있다.

보안은 지정된 정보, 물질, 인원, 활동 및 설비가 정탐, 파괴행위, 전복 및 테러에 대항하여 보호될 뿐 아니라 손실 또는 허가되지 않는 노출에 대해서도 보호되어지는 상태를 말한다.[44] 이는 보호해야 될 필요가 있다고 판단한 것들에 대하여 보안위협이 되는 외부의 침입으로부터 보호하는 것을 의미한다.

2) 보안위험성

보안위험성은 표적에 노출될 취약성 및 공격의 결과가 결부된 공격위협의 함수 작용이라고 ISPS Code에는 정의되어 있다. 이는 항만시설에 대해 발생 가능한 보안위협을 식별하고 이들 보안위협에 항만시설이 노출

44) 한국선급(KR), ISPS Code CSO/SSO Training Course 교재(Rev. 0), 2003, pp. part 1./17.

되어 있는 정도와 만약 보안위협이 발생하여 보안사고로 진전된다면 나타날 수 있는 피해 결과를 추정하여 상호 조합하는 일련의 프로세스가 수행되는 것을 의미한다.

3) 항만시설 보안평가

ISPS Code에는 항만시설 보안평가는 공격의 대상이 될 수 있거나 이러한 가능성이 더 높은 부분을 결정하기 위한 항만시설 운영의 모든 측면에서의 근본적인 위험성 분석이라고 정의되어 있다. 항만시설 운영의 모든 측면에서의 근본적인 보안위험성 분석이란 항만시설 운영의 전반적인 부분에 대하여 보안 상태를 확보할 수 있도록 보안에 대한 위험성 분석 즉 보안위험성의 상태를 체계적으로 확인하는 것이라고 할 수 있다.

3. 항만시설 보안평가 모델 구축

항만시설 운영에 대한 근본적인 보안위험성을 분석하는 것이 항만시설 보안평가라는 것을 앞에서 확인하였으며 보안위험성 분석은 보안위험성의 상태를 체계적으로 확인하는 것이라고 또한 확인하였다.

항만시설 보안평가를 통하여 항만시설 보안평가의 구성요소에 제시된 사항들을 도출하기 위해서는 보안사건이나 보안 사고를 발생시키는 다양한 원인인 보안위협요인을 파악하는 것부터 파악된 보안위협을 적절히 관리하기 위한 방법을 모색하는 것까지 전체적으로 분석하고 접근하여야 할 필요성이 있다는 것을 알 수 있다. 전체적인 분석과 접근을 위해서는 구체적인 기술적인 방법이 필요하다. 즉 항만시설 보안평가는 구체적인 기술적 방법을 적용하여 보안위험성을 평가하여야 한다.

안전에 대한 위험성 평가 방법론을 고찰하면서 다음과 같은 위험성 평가 방법의 특성을 확인할 수 있었다.

첫 째, 특정한 시스템이나 업무 수행 중에 내재되어 있는 위험을 규명하고 이것들을 평가하여 발생 가능한 사고나 재해의 특성을 파악하고 나아가 발생빈도와 재해 결과가지 예측하여 잠재된 위험으로부터 안전을 확보하기 위한 방안을 모색하는 체계적인 방법이 위험성 평가 방법이다.

둘 째, 대응 방안의 우선순위를 결정함으로서 제한된 자원을 효율적으로 사용할 수 있도록 방법을 제공하는 것은 위험성 평가가 가지는 큰 특징이라고 할 수 있다.

위의 위험성 평가 특성을 고찰하면 ISPS Code에서 요구하는 항만시설 보안

평가에 관한 요건과 같은 맥락을 가지고 있음을 알 수 있다. 그러므로 항만시설 보안평가를 시행하기 위하여 적용하는 구체적인 기술적 방법으로 안전 분야의 위험성 평가 방법을 모델로 적용하는 것이 타당한 방법이라고 할 수 있다.

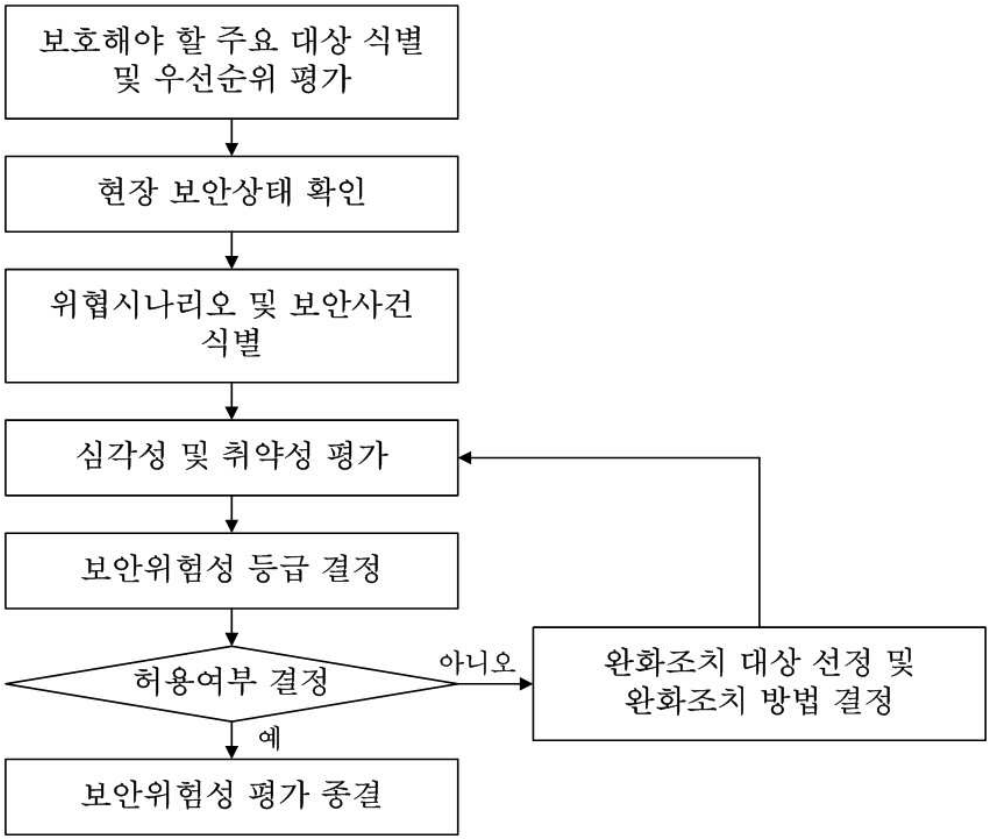
본 연구에서 설정한 위험성 평가 방법을 모델로 항만시설 보안평가 모델을 구축하면 <표 3-9>와 같이 구축할 수 있다.

<표 3-9> 위험성 평가 모델을 기준으로 구축한 항만시설 보안평가 모델

평가 단계	위험성 평가	항만시설 보안평가
1	운영 중인 시스템이나 수행 중인 작업에 대한 전개	보호해야 할 주요 대상 식별 및 우선순위 평가
2	위험 파악	현장보안상태 확인
3	발생 결과 평가	위협시나리오 및 보안사건 식별
4	빈도/가능성 평가	심각성 및 취약성 평가
5	위험성 산정 및 등급 결정	보안위험성 등급 결정
6	개선대책 수립	완화조치 대상 선정 및 완화조치 방법 결정
7	개선대책에 대한 위험성 재평가	보안위험성 재평가 및 완화조치 확정

<표 3-9>에 제시된 항만시설 보안평가 모델을 토대로 체계를 구성하면 다음과 같이 구성할 수 있다(<그림 3-5> 참조).

<그림 3-5> 항만시설 보안평가 체계도



제4장 항만시설 보안평가 모델의 적용

제3장에서는 위험성 평가 방법론을 근거로 항만시설 보안평가를 시행하기 위한 이론적인 방안과 항만시설 보안평가 모델이 제시되었다. 제3장에서 제시된 항만시설 보안평가의 모델을 토대로 각 단계별로 구체적으로 전개시키기 위한 방안이 필요하다. 이 장에서는 항만시설 보안평가를 수행하기 위한 각 단계별 세부 내용을 구체적으로 조명하고자 한다.

제1절 보호해야 할 주요대상 식별 및 우선순위 평가

1. 목적

보호해야 할 주요대상 식별 및 우선순위 평가는 다음과 같은 목적을 달성하기 위하여 실시한다.

(1) 항만시설 또는 항만시설 내의 시설물이나 기반시설의 기능을 명확하게 식별
(2) 보안위협이나 보안사건으로부터 보호하기 위한 항만시설 내의 시설물이나 기반시설을 식별
(3) 보호대상의 상대적 중요성에 대하여 우선순위를 결정
(4) 보안평가를 수행하기 위한 대상을 결정

2. 식별 및 평가 기준

1) 항만시설 내에 있는 주요 자산이나 기반시설들을 대상으로 보호해야 할 주요대상에 포함되는지 판단하기 위하여 먼저 대상 시설물이나 기반시설이 가지고 있는 기능이나 임무에 대하여 명확하게 규명하여야 한다. 시설물이나 기반시설의 기능이나 임무는 다음과 같이 구분하여 적용한다.
(1) 공공위생 측면의 기능
(2) 상업적 측면의 기능
(3) 공공안전 측면의 기능
(4) 운송 측면의 기능
(5) 통신 측면의 기능

(6) 기타

2) 다음으로 시설물이나 기반시설이 손상 또는 파괴되는 경우에 미치는 영향에 대하여 평가하여야 하며 미치는 영향은 다음과 같이 구분하여 적용한다.
   (1) 인명손상
   (2) 경제적 피해
   (3) 환경적 피해
   (4) 공공안전에 미치는 피해
   (5) 상징적 가치

3) 마지막으로 시설물이나 기반시설이 손상 또는 파괴되는 경우에 항만시설이 가지고 있는 고유 기능을 운영하는데 미치는 영향에 대하여도 평가하여야 하며 평가는 다음 두 가지 부분으로 나누어서 평가한다.
   (1) 항만시설 운영에 영향을 미치는 정도
   (2) 복구 능력의 정도
   (3) 복구 능력의 정도는 손상 또는 파괴된 시설물이나 기반시설을 반드시 원상 복구해야만 하는 것은 아니다. 다른 대체 수단이 있어서 항만시설의 고유 기능을 회복시킬 수 있는 경우에는 이를 복구 능력의 정도에 포함시켜서 평가하여야 한다.

3. 우선순위 평가 방법

우선순위 평가는 2 단계로 나누어서 진행한다. 먼저 시설물이나 기반시설이 가지고 있는 기능/임무와 시설물이나 기반시설이 파괴되는 경우 미치는 영향에 대한 평가와 항만시설 운영에 미치는 영향도와 복구 능력에 대한 평가를 각각 시행한 후 이 평가 결과를 다시 상호 평가하여 최종 우선순위를 결정한다.

1) 기능/임무와 대상이 파괴되는 경우에 미치는 영향에 대한 평가
   (1) 구분

<표 4-1> 기능/임무 및 대상이 파괴되는 경우에 미치는 영향에 대한 구분

기능 / 임무	대상이 파괴되는 경우에 미치는 영향
1.공공위생 측면 2.상업적 측면 3.공공안전 측면 4.수송 측면 5.통신 측면 6.기타	1.인명손상 2.경제적 피해 3.환경적 피해 4.공공안전 5.상징적 가치

(2) 기능/영향 평가 매트릭스

<표 4-2> 기능/영향 평가 매트릭스

미치는 영향 / 기능/임무	3개 이상	2개	1개 또는 없음
3개 이상	3	3	2
2개	3	2	1
1개 또는 없음	2	1	1
3: 중요도 높음, 2: 중요도 보통, 1: 중요도 낮음			

2) 항만시설 운영에 미치는 영향도와 복구 능력에 대한 평가

(1) 구분

<표 4-3> 항만시설 운영에 미치는 영향도 및 복구 능력 구분

항만시설 운영에 미치는 영향도	복구 능력
높음	높음
보통	보통
낮음	낮음

(2) 운영/복구 능력 평가 매트릭스

<표 4-4> 운영/복구 능력 평가 매트릭스

복구능력 / 운영측면	낮음	보통	높음
높음	3	3	2
보통	3	2	1
낮음	2	1	1
3: 중요도 높음, 2: 중요도 보통, 1: 중요도 낮음			

3) 보호해야 할 주요대상 우선순위 평가

(1) 평가 매트릭스

<표 4-5> 우선순위 평가 매트릭스

운영/복구능력 / 기능/영향	**3**	**2**	**1**
3	3	3	2
2	3	2	1
1	2	1	1
3: 우선순위 높음, 2: 우선순위 보통, 1: 우선순위 낮음			

4) 평가를 할 때 다음 사항은 주의 사항으로 고려되어야 한다.

(1) 동일한 기능을 동일한 기능을 수행하고 있는 시설물이나 기반시설이 여러 군데에 분산되어 있는 경우는 각 각에 대하여 중요도를 별도로 평가하지 않고 하나만 평가하여 공동으로 적용하는 것이 효과적이다. (예. 각 항만의 출입 Gate).

(2) 동일한 기능을 동일한 기능을 수행하고 있는 경우라도 시설물이나 기반시설을 운영하기 위하여 설치된 또는 시설물이나 기반시설에 부속하여 설치된 장치, 장비 또는 시스템이 현저하게 차이가 나는 경우에는 별도로 분리하여 식별하고 평가하여야 한다.(예. 각 항만의 출입 Gage 중에서 통신 케이블, 교통통제 시스템이 설치된 Gate의 경우 다른 Gate와 다는 기능을 수행하고 있으므로 별도로 분리하여 중요도를 평가하여야 한다.)

4. 우선순위 평가결과에 대한 관리

평가 결과 등급이 3 및 2로 나온 시설물이나 기반시설은 보호해야 할 주요 대상으로 식별하여야 하며 반드시 보안위험성 평가를 시행하여야 하는 대상에 포함시켜야 한다.

제2절 현장보안상태 확인

1. 목적

현장보안상태 확인은 다음과 같은 목적을 달성하기 위하여 시행한다.

1) 항만시설 또는 항만시설 내의 시설물이나 기반시설에 대한 현재의 보안상태를 파악한다.
2) 향후 완화조치를 시행할 경우 완화조치 방법을 결정하기 위한 근거를 제공한다.
3) 현재의 보안상태를 각 평가 항목별 기준에 따라 평가하여 보안수준을 확인한다.

2. 현장보안상태 확인 방법

1) 현장보안상태 확인에서 확인해야 할 대상으로 고려하여야 하는 것은 다음과 같다.
   (1) 보안절차
   (2) 보안조직
   (3) 보안장비 및 보안시스템
   (4) 보안 임무 수행자들의 업무 능력 정도

보안절차를 확인할 때는 항만시설의 보안 업무와 관련하여 현재 적용되고 있는 모든 규정들을 조사하여 확인하고 검토한다. 여기에는 강제적으로 적용되는 법규뿐만 아니라 항만시설 자체에서 수립한 절차 및 보안관련 유관기관에서 수립하여 시행 중에 있는 여러 지침 중에서 항만시설에 적용되는 사항도 빠짐없이 모두 조사되고 검토되어야 한다. 특히 비상대응과 관련하여 유관기관 간 그리고 유관기관과 항만시설간의 책임과 의무를 나타내고 있는 비상대응계획은 반드시 검토한다.

2) 현장보안상태 확인을 효과적이고 효율적으로 하기 위하여 점검 표를 구성하는 것이 필요하다. 점검 표를 구성하는 원칙은 ISPS Code A편 제14.2절에 규정되어 있는 7개 항목을 대분류 기준으로 설정하고 ISPS Code B편의 항목들을 해당되는 대분류 밑에 배치하여 구성하는 것이다. 이렇게 구성된 점검 표는 현장보안상태 확인을 함과 동시에 항만시설이 ISPS Code를 이행하기 위하여 필요한 사항들이 어떤 것인지를 쉽게 식별할 수 있도록 한다.

   ISPS Code A편 제14.2절에 규정된 사항은 다음과 같다.

   (1) 항만시설 보안임무 수행
   (2) 접근 통제
   (3) 항만시설 감시(모니터링)
   (4) 제한구역 감시(모니터링)
   (5) 화물취급 감독
   (6) 선용품 취급 감독
   (7) 용이한 보안통신 이용

3) 시설물 또는 기반시설에 대한 현장보안상태 확인을 할 때는 우선순의 평가 등급이 3(높음)과 2(보통)로 식별된 주요 대상에 대하여만 적용한다.

4) 현장보안상태 확인은 현재 시행 또는 적용되고 있는 보안활동이나 보안장비 및 보안시스템만을 반영하여야 한다. 향후에 시행 또는 적용하기로 예정되어 있는 사항들은 포함시키지 말아야 한다.

제3절 위협 시나리오 및 보안사건 식별

1. 목적

위협 시나리오 및 보안사건 식별은 다음 목적을 달성하도록 시행한다.

1) 보호해야 할 필요가 있다고 식별된 주요 대상에 대하여 위협을 줄 수 있는 보안위협을 식별한다.
2) 식별된 보안위협이 사건으로 전개될 때 발생할 수 있는 보안사건에 대한 시나리오를 파악한다.

즉 항만시설의 주요 대상에 내재되어 있는 보안위험요소를 식별하기 위한 것이다.

2. 식별방법

1) 위협 시나리오 및 보안사건을 식별할 때 다음 사항을 고려하여 식별한다.
   (1) 과거에 발생했던 보안사건
   (2) 보안관계기관과의 협의 또는 자문
   (3) 이미 제정되어 있는 보안관련 강제 규정

2) 위협 시나리오 및 보안사건을 식별할 때 제1단계에서 식별된 주요 대상 중 우선순위 등급이 2(보통) 이상으로 식별된 대상별로 발생 가능성이 있는 위협 시나리오 및 보안사건을 확인하여야 한다.

3) ISPS Code B편 제15.11항에 제시된 발생 가능성이 있는 보안사건을 포함하여 발생 가능한 위협 시나리오 및 보안사건을 전개하면 다음과 같은 사항들을 식별할 수 있다(<표 4-6> 참조).

<표 4-6> 발생 가능성이 있는 위협 시나리오 및 보안사건의 예

보안시나리오		적용 예
대분류	**중분류**	
1. 침입, 주요 대상 점유	1.1 침입, 주요 대상 점유 : 폭발물에 의한 손상 및 파괴	폭발물 설치
	1.2 침입, 주요 대상 점유 : 악의적인 작동 및 행위에 의한 손상/파괴	선박 탈취, 고의 좌초 및 충돌 고의 밸브개방.(위험물 유출 등)
	1.3 침입, 주요 대상 점유 : 주요 대상을 파괴하지 않고 위험물사고 또는 오염사고 유발	밸브/밴트 개방(독극물 유출) 안전장치 해제(손상 및 파괴 유발)
	1.4 침입, 주요 대상 점유 : 인질 납치, 살인	살인
2. 외부 공격	2.1 주요 대상(target)에 인접한 해상, 육상 또는 수중으로부터 폭발물을 이용한 공격	승용차 및 트럭에 의한 폭발.
	2.2 선박 또는 차량을 고정시설물에 충돌시키는 공격	고의적인 충돌(항만시설 운영에 대한 손상/파괴/중지가 목적)
	2.3 원거리에서 무기를 발사	미사일과 총 등에 의한 공격
3 밀수입, 밀반출	3.1 불법 무기 또는 폭발물의 밀반입·밀반출	무기 및 장비의 밀수 (대량살상무기 포함)
	3.2 밀입국 또는 밀항	밀항 또는 밀입국
4. 사이버 조작	4.1 항만시설 또는 선박의 전산 시스템 조작(항만운영을 중단시키거나 불법 활동을 조장할 목적)	항만시설의 화물서류파일 해킹(고가화물이 적재된 컨테이너 식별 목적) 유류이송관리 컴퓨터 시스템 해킹(저장탱크의 유류를 넘치게 할 목적)

<표 4-6> 발생 가능성이 있는 위협 시나리오 및 보안사건의 예(계속)

보안시나리오		적용 예
대분류	**중분류**	
5. 화물 등의 조작	5.1 화물, 선박의 주요 설비 또는 시스템, 선용품 등의 조작(위해상황을 만들 목적)	선적될 화물에 화학반응을 일으키는 물질 첨가 운송 중에 화물이 떨어지도록 록 조작 컨테이너나 화물 고박장치를 약화시켜 이송 중에 떨어지도록 함 화물 원산지 변경(파괴하기 위한 장비를 밀수할 목적으로 정부의 검사를 피하거나 줄이기 위함) 유해 또는 손상을 유발하는 화물의 등급 변경
6. 무허가 사용	6.1 운영 목적이외에 선박 또는 부두시설에 대한 무허가 사용	허가되지 않은 직원에 의한 무허가 화물 양하
7. 항만 접근로 등의 봉쇄	7.1 항만입구, 갑문, 접근로 등의 봉쇄	갑문 탈취 및 봉쇄
8. 평가를 수행하는 보안전문가 또는 항만시설관리자에 의해 추가된 기타 시나리오		

4) 위협 시나리오 및 보안사건을 식별할 때 다양한 경우를 가정하여 식별하여야 하나 너무 많은 종류나 최악의 경우를 고려한 시나리오까지 고려할 필요는 없다.

제4절 심각성 및 취약성 평가

1. 목적

식별된 보안사건이 발생된 경우 미치는 영향(심각성) 및 발생할 수 있는 가능성(취약성)을 평가한다.

2. 평가방법

1) 심각성 및 취약성을 평가할 때 다음 사항들을 고려하여서 평가에 반영하도록 한다.
   (1) 과거에 발생한 보안사건
   (2) 보안관계기관과의 협의 또는 자문
   (3) 이미 제정된 보안관련 규정
   (4) 2단계에서 시행한 현장보안상태

2) 3단계에서 식별된 시나리오별로 시나리오가 발생될 경우 미치는 영향을 가정하여 평가기준에 따라 평가한다.

3) 취약성을 평가할 때는 2단계 현장보안상태 확인에서 평가한 현재의 보안상태를 감안하여 평가한다. 즉 현재 적용 또는 시행되고 있는 보안절차나 보안장비 또는 보안시스템을 고려하여 발생가능성을 평가한다. 시나리오가 발생할 가능성 즉 취약성은 두 부분으로 구분하여 평가를 시행한다. 보안위협을 하는 조직이 외부로부터 접근하는 정도를 평가하는 외부로부터의 접근용이성과 내부조직이 외부 침입을 감지할 수 있는 정도를 평가하는 보안조직성으로 구분하여 평가를 시행한다. 두 부분의 평가 결과를 종합한 것이 취약성 평가 결과이다.

4) 심각성 및 취약성 평가 기준은 다음과 같이 적용한다.
   (1) 심각성 평가 기준

<표 4-7> 심각성 평가 기준

범주 \ 등급	높음(3점)	중간(2점)	낮음(1점)
사망/부상	○대량 인원의 사망 및 심각한 부상	○상당한 인원의 사망 및 심각한 부상	○약간명의 사망 및 심각한 부상
경제영향	○심각한 경제적 피해	○상당한 경제적 피해	○미미한 경제적 피해
환경영향	○대규모 지역에 걸친 다양한 측면의 생태계 파괴 예: 국가적 재난대책본부가 설치되어야 하는 정도	○생태계의 일정부분에 대한 장기간의 손상 예: 지역방제대책본부가 설치되어야 하는 정도	○생태계에 약간의, 국지적인 영향을 주는 소규모의 유출
국가방위	○공공안전 및 방위에 치명적이고 장기간에 걸친 취약점 노출 예: 항만종합전산망의 장기간 붕괴	○공공안전 및 방위에 단기간에 걸친 취약점 노출 예: 항만종합전산망의 해킹 항만관제탑 파괴	○사소한 영향
상징적 효과	○국가적으로 중요하고 국제적으로 알려진 상징물의 손실 예: 여객터미널의 파괴	○지역적으로 중요한 상징물의 손실 예: 항만관제탑의 파괴, 하역크레인 파괴	○사소한 손상

(2) 2가지 이상의 복합적인 범주에서 피해가 발생하는 경우에는 각각의 범주에 대한 등급을 부여하고 그 중에서 가장 최상위 등급으로 심각성의 등급을 결정한다.

예. 사고가 발생하면 심각한 경제적 피해(높음:3점)를 미치고 지역적으로 중요한 상징물의 손실(중간:2점)이 발생하는 심각성인 경우에 높음(3점)으로 심각성 등급을 결정함.

(3) 취약성 평가 기준

취약성은 접근용이성과 보안조직성 두 부분으로 구분하여 등급을 결정한다. 접근용이성은 물리적이며 지리적인 장애물이 있어서 보안조직의 활동과 관계없이 외부침입자가 접근을 할 수 없도록 하는 것이며, 보안조직성은 보안조직의 활동으로 인하여 외부침입자가 침입을

할 수 없도록 하는 것으로 구성된 보안조직, 통신체제, 보안절차, 침입탐지시스템 등을 말한다(<표 4-8> 참조).

<표 4-8> 취약성 평가 기준

등급 / 범주	높음(3점)	중간(2점)	낮음(1점)
접근 용이성	○ 저지 능력이 없음(즉, 대상에 대한 접근이 제약되지 않으며 내부활동도 제한되지 않음.)	○ 양호한 저지(즉, 실제적인 장애가 하나 있음; 목표물 50m까지의 접근은 제한되지 않음.) 예: 정문에서는 검색되나 관제탑에서는 검색 없음.	○ 뛰어난 저지(공격에 대해 저지 가능함; 대상의 200m이내의 접근은 제한됨; 다중의 물리적/지정학적 장벽이 있음)
보안 조직성	○ 시기적절한 방어를 위한 저지 능력이 없으며(즉, 계획, 경비인력, 비상통신, 외부 공권력이 없음), 탐지능력이 없음.	○ 양호한 저지능력(즉, 최소의 보안계획, 약간의 통신시설과 목표에 비해서 제한된 규모의 무장경비인력; 외부 공권력이 적기의 방어를 위해 유용하지 않으며, 제한된 탐지시스템이 있음.)	○ 공격을 저지할 수 있을 것으로 기대되는 뛰어난 저지능력; 보이거나 외관으로 드러나지 않는 추가요소들을 나타내는 은밀한 보안요소들

(4) 취약성은 접근용이성의 평가 점수와 보안조직성의 평가 점수를 합한 것으로 결정한다.

예. 접근용이성이 중간(2점)으로 평가되었고 보안조직성이 낮음(1점)으로 평가된 경우 취약성은 3점이 됨.

(5) 심각성 및 취약성의 등급을 부여할 때는 너무 과장되거나 또는 축소하여 부여하지 않도록 하여야 하며, 취약성은 현장보안상태 확인에서 식별된 사항을 반드시 반영하여 접근 용이성 및 보안 조직성을 평가하여야 한다.

제5절 보안위험성 등급 평가

1. 목적

식별된 시나리오가 발생된 경우의 보안위험성 등급을 결정하고 완화조치가 필요한지를 확인한다.

2. 평가 방법

1) 보안위험성 등급 평가는 식별된 시나리오가 발생된 경우에 대한 심각성 등급과 취약성 등급을 기준으로 위험성 등급을 산정한다.

2) 보안위험성 등급 평가 매트릭스

<표 4-9> 보안위험성 등급 평가 매트릭스

		취약성 등급(vulnerability level)		
		5-6	3-4	1-2
심각성 등급 (consequence level)	3	완화조치필요	완화조치필요	완화조치검토
	2	완화조치필요	완화조치검토	현재조치유지
	1	완화조치검토	현재조치유지	현재조치유지

예: 심각성 등급이 2이고 취약성 등급이 5인 경우에 보안위험성은 3등급 완화조치 필요가 됨.

3) 보안위험성 등급은 3등급으로 구분하여 평가한다.

(1) 1등급 : 현재조치유지

현재의 보호조치를 유지하면 되는 상태로, 평가결과를 자료로 정리하여 필요시 사용할 수 있도록 보관하면 되는 상태

(2) 2등급 : 완화조치검토

상황에 따라 추가적인 보호조치가 개발되어야 하는 상태

(3) 3등급 : 완화조치필요

높은 상태의 위험이 예상되며, 위험을 감소시키기 위하여 추가적인 보호조치 또는 절차의 개발이 필요한 상태

제6절 완화조치 대상 선정 및 완화조치 방법 결정

1. 목적

이 단계에서는 보안위험성 등급을 평가한 결과를 바탕으로 완화조치를 해야 할 필요성이 있는 부분을 식별하고, 완화조치가 필요한 부분에 대하여는 적절한 완화조치가 어떤 것인지 식별하는 것을 목적으로 한다.

2. 시행방법

1) 완화조치 대상이 되는 시나리오는 다음과 같다.
   (1) 보안위험성 등급이 완화조치필요로 식별된 모든 시나리오
   (2) 보안위험성 완화조치검토로 식별된 시나리오 가운데 주요 대상의 중요도가 높음으로 평가된 것
   (3) 기타 완화조치가 필요하다고 판단한 시나리오

2) 완화조치 대상이 되는 시나리오에 대하여는 보안위험성을 낮추기 위한 적절한 방법을 파악하여야 한다. 완화방법을 파악하기 위해서는 관계 기관과의 협의 또는 항만운영 및 보안에 경험이 있는 책임자들로 팀을 구성하고 브레인스토밍 방법을 통하여 적용가능성이 있는 모든 방법을 식별하여야 한다.

3) 적용가능성이 있다고 파악된 완화조치방법은 취약성을 감소시키는 것인지 심각성을 감소시키는 것인지 구분을 한다.

4) 적용가능성이 있다고 파악된 완화조치방법은 우선순위를 결정하기 위하여 효과성과 실행가능성 관점에서 평가를 하여 우선순위를 결정하고 채택여부를 확정하여야 한다.

5) 호과성은 다음과 같이 구분하여 평가한다.
   (1) 효과성 있음 : 완화조치를 단독적으로 시행하는 경우 심각성 또는 취약성 점수를 낮출 수 있다고 판단되면 효과성이 있는 것으로 판단
   (2) 효과성 부분적 : 하나 이상의 다른 전략과 함께 시행되었을 때 점수를 낮출 수 있다면 효과성이 부분적으로 있는 것으로 판단

(3) 효과성 없음 : 시행하여도 점수를 낮추지 못한다고 예상이 되면 효과가 없는 것으로 판단

6) 실행 가능성은 다음과 같이 구분하여 평가한다.
(1) 실행 가능성 있음 : 약간의 어려움으로 또는 현재의 예산제한 내에서 시행될 수 있다면 실행 가능성 있음으로 판단
(2) 실행 가능성 부분적 : 하나 이상의 다른 전략과 함께 시행되었을 때 점수를 낮출 수 있다면 효과성이 부분적으로 있는 것으로 판단
(3) 실행 가능성 없음 : 그것의 실행이 의문시되거나 극도의 위협상황이 아니라면 실행비용을 쓸 수 없다면 실행가능성이 없는 것으로 판단

7) 완화조치 방법을 결정할 때는 효과성과 실행 가능성을 복합적으로 평가하여 결정한다. 또한 심각성 등급을 낮추는 방법보다 취약성 등급을 낮추는 방법을 먼저 고려하는 것이 필요하다. 이는 일반적으로 심각성을 낮추는 방법은 시간적으로 많은 시간이 소요되며 비용도 많이 투자되고 기술적으로도 당장 해결하기가 쉽지 않은 것들일 수가 있기 때문이다.

제7절 보안위험성 재평가 및 완화조치 확정

1. 목적

6단계에서 결정된 완화조치가 실질적으로 보안위험성 등급을 낮추는 것인지 확인하고, 확정된 경우에는 항만시설보안시스템에 반영하기 위함을 목적으로 보안위험성 재평가를 시행한다.

2. 재평가 시행 방법

1) 6단계에서 결정된 완화조치를 심각성 및 취약성 평가 단계에서 다시 대입하여 평가를 시행하고 실질적으로 심각성이나 취약성이 낮아지고 그 결과 보안위험성 등급이 필요한 만큼 완화되는지 재평가를 시행한다.

2) 재평가 결과 보안위험성 등급이 완화되지 않으면 이 완화조치는 채택하지 않으며 추가의 완화조치를 고려하거나 별도의 완화조치를 식별하여 보안위험성을 재평가 하여야 한다.

3) 재평가 결과 보안위험성 등급이 허용되는 수준까지 완화되는 경우에는 이 완화조치를 채택하고 항만시설보안시스템에 반영하기 위한 계획을 수립하여야 한다.

제8절 항만시설 보안평가 실제 적용 사례

본 연구에서 구축된 항만시설 보안평가 모델을 실제로 적용하여 항만시설 보안평가를 시행한 결과는 다음과 같다.

1. 대상 항만시설

부산항에 위치한 000 컨테이너 전용터미널을 대상으로 한다. 이 터미널을 이용하는 선박들의 주요 항로는 미주, 유럽, 동남아, 지중해, 아프리카, 남미, 호주, 중국 등이다.

이 터미널은 안벽의 길이가 1,200 미터이고, 수심이 14-15 미터이며, 총 면적이 1,038,803 평방미터이다. 터미널은 CY, CFS를 가지고 있고 철송을 하기 위하여 철도가 연결되어 있다.

2. 항만시설 보안평가

1) 보호해야 할 주요 대상 및 우선순위 식별

보호해야 할 주요 대상을 식별하고 주요 대상들에 대한 기능 및 파괴되는 경우에 미치는 영향, 그리고 파괴되는 경우에 항만시설 운영에 미치는 영향 및 복구 능력을 평가하면 다음과 같다(<표 4-10> 참조).

<표 4-10> 보호해야 할 주요 대상의 각 부문에 대한 평가표

대상	기능 / 임무	대상이 파괴되는 경우에 미치는 영향	복구 능력	운영측면 영향도
	1. 공공위생 2. 상업 3. 공공안전 4. 수송 5. 통신 6. 기타	1. 인명손상 2. 경제적 영향 3. 환경적 영향 4. 공공안전 5. 상징적 영향	1.높음 2.보통 3.낮음	1.낮음 2.보통 3.높음
변전실	2 / 3	2 / 3 / 5	1	3
C / C	2 / 4	2 / 5	1	3
위험물장치장	3	3 / 4	3	2
비상발전소	2 / 3	2 / 4	2	2
위험물 옥외 저장소	1 / 3	3 / 4	2	2
자가 주유소	3 / 4	2 / 3	2	2
운영건물(컨트롤 센터, 전산실)	2 / 3 / 4 / 5	1 / 2 / 4 / 5	3	3
항로 및 항로표지	2 / 3 / 4	2 / 4 / 5	2	3
묘박지	4	5	1	1
항만시설에 인접한 수역	6	5	1	1
PTMS	3 / 5	1 / 4 / 5	2	3
역무선 (항내서비스)	6	4	1	1
T / C	2 / 4	2 / 4	2	1
이동장비	2 / 4	2 / 5	2	1
접안시설(선석)	2 / 4	2 / 4	2	3
CY	2 / 4	2 / 5	1	3
GATE	2 / 4	1 / 2	2	2
합동초소 (보안감시시스템)	3 / 5	1 / 4	2	2
철송장(철로)	2 / 4	2 / 5	2	2
냉동장치장	2 / 4	1 / 3	2	2
CSI 검색기	1 / 3	1 / 3	2	2
창고CFS	2 / 4	1 / 2	2	2
LB1, LB2, LB3 복합건물	1 / 6	1 / 5	1	1

보호해야 할 주요 대상의 각 부문에 대한 평가를 근거로 기능/영향 평가 매트릭스와 운영/복구 능력 평가 매트릭스에 따른 평가를 거친 후 우선순위 평가 매트릭스에 따라 우선순위를 평가하여 우선순위가 보통이상으로 평가된 것을 구성하면 다음과 같다(<표 4-11> 참조).

<표 4-11> 주요대상의 우선순위 평가표

번호	주요 대상 명	우선순위
1	변전실	3
2	PTMS	3
3	운영건물(컨트롤 센터, 전산실)	3
4	항로 및 항로표지	3
5	접안시설(선석)	3
6	자가 주유소	2
7	C / C	2
8	냉동장치장	2
9	CSI 검색기	2
10	창고(CFS)	2
11	비상발전소	2
12	위험물옥외저장소	2
13	위험물장치장	2
14	CY	2
15	GATE	2
16	합동초소 (보안감시시스템)	2
17	철송(철로)	2

2) 보안위험성 등급 평가

우선순위가 2 이상인 주요대상에 대하여 발생 가능한 위협 시나리오 및 보안사건을 식별하고 현장 보안상태를 통하여 확인한 현재의 보안조치를 감안하여 심각성 및 취약성 평가하여 보안위험성 등급을 평가하면 다음

과 같다(<표 4-12> 참조).

3) 완화조치 대상 선정 및 완화조치 방법 결정

완화조치가 필요한 대상에 대하여 적용 가능한 완화조치 방법을 선정하고 선정된 완화조치 방법에 대하여 효과성과 실행가능성을 평가하여 채택 여부를 판정하면 다음과 같다(<표 4-13> 및 <표 4-14> 참조).

4) 보안위험성 재평가 및 완화조치 확정

채택된 완화조치가 실질적으로 보안위험성을 완화시키는지 확인하기 위한 보안위험성 재평가를 시행하면 다음과 같다(<표 4-15> 참조).

<표4-12> 보안위험성 등급 평가표(1/17)

주요 대상명 : 철송(철도) 우선순위 : 2

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
테러분자에 의한 철도 레일 폭파	진입로 철도 운송 시스템 적용	출입자 검문 검색	해당 없음	해당 없음	해당 없음	24시간 청경 감시 및 순찰	2	1	1	2	2•2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(2/17)

주요 대상명 : 냉동장치장 우선순위 : 2

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
항만시설 내에 침입하여 냉동장치장 파괴	별도의 장벽이나 폐쇄장치	출입자 검문검색	해당 없음	해당 없음	해당 없음	24시간 청경감시 및 순찰	2	1	1	2	2•2 현재 조치 유지	
외부차량 돌진으로 파괴	별도의 장벽이나 폐쇄장치	출입자 검문검색	해당 없음	해당 없음	해당 없음	24시간 청경감시 및 순찰	2	1	1	2	2•2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(3/17)

주요 대상명 : CSI 검색기 우선순위 : 2

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
항만시설 내에 침입하여 CSI 검색기 파괴	· 제한 구역으로 지정 · 보안 울타리 설치	· 2중 검문 검색 · 출입자 안내 통제	컨테이너 내장화물의 검색	해당 없음	해당 없음	청경 24시간 근무	2	1	1	2	2 • 2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(4/17)

주요 대상명 : 합동초소(보안감시 시스템) **우선순위 : 2**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
항만시설 내에 침입하여 합동초소 파괴	정문 초소 내에 설치	24시간 청원경찰 배치	해당 없음	해당 없음	해당 없음	· 24시간 고정 감시 · 부분적으로 감시 초소 설치	1	1	1	2	1•2 현재 조치 유지	
외부차량 돌진에 의한 통제 시스템 파괴	정문 초소 내에 설치	안전 바리 게이트 설치	해당 없음	해당 없음	해당 없음	· 24시간 고정 감시 · 부분적으로 감시 초소 설치	1	1	1	2	1•2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(5/17)

주요 대상명 : GATE 우선순위 : 2

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
컨테이너 운송 차량의 돌진에 의한 파괴	보호 구역으로 지정	컨테이너 차량 필요시 검문검색	해당 없음	해당 없음	해당 없음	2차 감시	1	3	1	4	1•4 현재 조치 유지	
침입자에 의한 보안시설 파괴	보호 구역으로 지정	출입인원 검문검색	해당 없음	해당 없음	해당 없음	2차 감시	1	3	1	4	1•4 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(6/17)

주요 대상명 : PTMS **우선순위 : 3**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
침입자에 의한 폭발물 설치 및 파괴	· 통제 구역 지정 · 2중 보안 울타리 설치	허가자만 출입, 그 외는 출입통제 및 안내	해당 없음	해당 없음	해당 없음	외곽에 현역 군인 감시 및 순찰	2	1	1	2	2●2 현재 조치 유지	
원거리에서 미사일 등으로 목표물 공격	〃	〃	해당 없음	해당 없음	해당 없음	외곽에 현역 군인 감시 및 순찰	2	1	1	2	2●2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(7/17)

주요 대상명 : 항로 및 항로 표시 **우선순위 : 3**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
대형 선박을 항로에 침몰	· 항로 표시 · 부표 표시	입항 24시간 전에 입항 예고 및 입항 즉시 입항 신고	해당 없음	해당 없음	해당 없음	· PTMS 시스템으로 감시 · 해경순찰선에 의한 감시 · 해군3함대의 레이더에 의한 감시	3	2	1	3	3 • 3 완화 조치 필요	예
선박으로 항로 표지 파손	개항 단속반 운영	개항 단속반 운영	해당 없음	해당 없음	해당 없음	개항 단속반 운영	1	2	1	3	1 • 3 현재조치유지	

<표4-12> 보안위험성 등급 평가표(8/17)

주요 대상명 : 운영건물(컨트롤 센터, 전산실) **우선순위 : 3**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
항만시설 내에 침입하여 운영 건물 파괴	별도의 장벽이나 폐쇄장치 설치	차량에 대한 진입허가 식별 청경 24시간 근무	해당 없음	해당 없음	해당 없음	CCTV 설치	3	1	1	2	3 • 2 완화 조치 검토	아니요
컨트롤 센터 및 전산실 사이버조작	방호프로그램 설치		해당 없음	해당 없음	해당 없음	인력순찰	2	1	1	2	2 • 2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(9/17)

주요 대상명 : 위험물 옥외 저장소 **우선순위 : 2**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
항만시설 내에 침입하여 위험물 옥외저장소 파괴	별도의 장벽이나 폐쇄 장치가 있음	허가자만 출입가능	해당 없음	해당 없음	해당 없음	청경 24시간 근무	2	1	1	2	2•2 현재 조치 유지	
테러를 위한 위해물질 절도	별도의 장벽이나 폐쇄 장치가 있음	허가자만 출입가능	해당 없음	해당 없음	해당 없음	청경 24시간 근무	2	1	1	2	2•2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(10/17)

주요 대상명 : 비상발전소 **우선순위 : 2**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
항만시설 내에 침입하여 비상발전소 파괴	별도의 장벽이나 폐쇄장치가 없음	차량에 대한 진입허가 식별되지 않음	해당 없음	해당 없음	해당 없음	· CCTV 설치 · 인력순찰 · 책임자 24시간 근무	2	1	1	2	2 • 2 현재 조치 유지	
연료탱크 조작으로 비상발전 불능 조작	별도의 장벽이나 폐쇄장치가 없음	차량에 대한 진입허가 식별되지 않음	해당 없음	해당 없음	해당 없음	· CCTV 설치 · 인력순찰 · 책임자 24시간 근무	2	1	1	2	2 • 2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(11/17)

주요 대상명 : 창고(CFS) **우선순위 : 2**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
선적화물에 누출을 유도하여 혼적 화물과 화학반응을 일으켜 운송 중 폭발 또는 화재 발생	보호 구역으로 지정	출입문에서 검문 검색	출입화물을 보세화물 규정에 따라 보세사 감독하에 화물 입출고 함	해당 없음	해당 없음	화물을 적제 또는 적출시 보세사의 감독 및 확인	2	1	1	2	2 • 2 현재 조치 유지	
안보위해 물품을 일반화물에 은닉 반출하여 사회혼란 조장	보호 구역으로 지정	출입문에서 검문 검색	출입화물을 보세화물 규정에 따라 보세사 감독하에 화물 입출고 함	해당 없음	해당 없음	화물을 적제 또는 적출시 보세사의 감독 및 확인	2	1	1	2	2 • 2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(12/17)

주요 대상명 : 위험물 장치장 **우선순위 : 2**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
항만시설 내에 침입하여 위험물 장치장 파괴	제한 구역 지정	차량에 대한 진입허가 식별되지 않음	해당 없음	해당 없음	해당 없음	· CCTV 설치 · 인력순찰 · 책임자 24시간 근무	2	1	1	2	2 • 2 현재 조치 유지	
테러를 위한 위해물질 절도	제한 구역 지정	차량에 대한 진입허가 식별되지 않음	해당 없음	해당 없음	해당 없음	· CCTV 설치 · 인력순찰 · 책임자 24시간 근무	2	1	1	2	2 • 2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(13/17)

주요 대상명 : 접안시설 **우선순위 : 3**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
해상에서 대형선박을 이용하여 선박 접안시설 파괴	선석 지정	· 선석 배정 · 입항 예보 및 입항 신고	해당 없음	해당 없음	해당 없음	· 해경 감시선에 의한 감시 · 해군 3함대 레이더의 감시	2	2	1	3	2•3 완화 조치 검토	아니오
출입자가 선용품에 폭발물을 은닉하여 항만에 반입하여 항만 시설 파괴	보안 울타리 설치	· 초소에서 출입자 및 차량 검문 검색 · 인력 순찰	게이트에서 외관 검사	선용품 허가서 확인 후 검색	해당 없음	CCTV에 의한 감시	2	1	1	2	2•2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(14/17)

주요 대상명 : C / C　　우선순위 : 2

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
자연재해(태풍 등)에 의한 파손	보호 구역내 설치	출입자 및 출입차량 출입증 소지 및 검문검색	화물장치장에 장치화물 봉인상태 확인	선용품 검색 수단 없음	해당 없음	· CCTV 설치 · 인력순찰 · 책임자 24시간 근무	2	1	1	2	2 • 2 현재 조치 유지	
외부침입자에 의한 파손	보호 구역내 설치	〃	〃	〃	〃	〃	2	1	1	2	2 • 2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(15/17)

주요 대상명 : 변전실 **우선순위 : 3**

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
항만시설 내에 침입 변전실 파괴 및 외부에서 폭발물 투척으로 인한 파괴	별도의 장벽이나 폐쇄장치 설치	허가자만 출입 그 외는 출입자 안내	해당 없음	해당 없음	해당 없음	인력 순찰	2	1	1	2	2 • 2 현재 조치 유지	
하역장비 (차량)에 의한 돌진으로 파괴	별도의 장벽이나 폐쇄장치 설치	허가자만 출입 그 외는 출입자 안내	해당 없음	해당 없음	해당 없음	인력 순찰	2	1	1	2	2 • 2 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(16/17)

주요 대상명 : 자가 주유소 우선순위 : 2

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
침입자에 의한 폭발물 설치 및 파괴	외곽 보안 울타리 설치	출입자 검문 검색	해당 없음	해당 없음	해당 없음	부두 내 순찰계획에 의한 순찰 및 감시	1	2	1	3	1•3 현재 조치 유지	
주유차량 방화로 인한 파괴	외곽 보안 울타리 설치	출입자 검문 검색	해당 없음	해당 없음	해당 없음	부두 내 순찰계획에 의한 순찰 및 감시	1	2	1	3	1•3 현재 조치 유지	

<표4-12> 보안위험성 등급 평가표(17/17)

주요 대상명 : CY 우선순위 : 2

식별된 시나리오	현재의 보안상태						심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 적용
	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시		접근 용이성	보안 조직성	취약성 결과		
안보위해물품을 일반화물에 은닉. 반출하여 사회혼란 조장	보호 구역으로 지정	출입문에서 검문 검색	출입화물을 보세화물 규정에 따라 보세사 감독하에 화물 입출고 함	해당 없음	해당 없음	부두 정문에서 화물 반출증 확인	2	1	1	2	2•2 현재 조치 유지	
외부침입자 또는 내부자에 의한 방화.	보호 구역으로 지정	출입문에서 검문 검색	출입화물을 보세화물 규정에 따라 보세사 감독하에 화물 입출고 함	해당 없음	해당 없음	순찰 계획에 의한 감시 순찰	2	1	1	2	2•2 현재 조치 유지	

<표4-13> 적용 가능성 있는 완화조치

주요 대상명: 항로 및 항로표지

식별된 시나리오	적용 가능성 있는 완화조치						위험성 감소대상	
	제한구역	접근통제	화물취급	선용품 인도	미휴대 수화물	감시	취약성	심각성
대형선박을 항로에 침몰시킴 (사고지점 N35°5′12″ E125°06′50″)						고성능 순찰선 고정배치	o	
	침몰선박 인양 시까지 항로 변경 : 입항 N35°05′18″, E129°06′57″, 출항 N35°05′06″, E129°05‘48“							o

<표4-14> 적용 가능성 있는 완화조치 평가

주요 대상명: 항로 및 항로표지

식별된 시나리오: 대형선박을 항로에 침몰시켜 항로 마비

구분	효과성			실행가능성			채택 여부
	예	부분적	아니오	예	부분적	아니오	
고성능 순찰선 고정 배치		O				O	불채택
항로변경		O		O			채택

<표4-15> 보안위험성 재평가

주요 대상명 : 항로 및 항로표지 **우선순위 : 3**

식별된 시나리오	제한 구역	접근 통제	화물 취급	선용품 인도	미휴대 수화물	감시	심각성 (Consequences)	취약성(Vulnerability)			보안 위험성	완화 조치 시행
								접근 용이성	보안 조직성	취약성 결과		
대형 선박을 항로에 침몰	· 항로 표시 · 부표 표시	입항 24시간 전에 입항예고 및 입항 즉시 입항 신고	해당 없음	해당 없음	해당 없음	· PTMS 시스템으로 감시 · 해경 순찰선에 의한 감시 · 해군 3함대의 레이더에 의한 감시.	1	2	1	3	1 • 3 현재조치유지	예
	선박항로 변경											

제5장 결론

제1절 연구결과의 요약

본 연구에서는 항만시설이 ISPS Code에서 요구하는 보안시스템을 제대로 수립하기 위해서는 보안시스템 수립에 선행하여 시행하는 보안평가를 정확히 실시하여야 하며 보안평가를 정확히 실시하기 위해서는 보안평가를 하는데 적절한 방법론이 필요하다는 것을 알 수 있었다.

적절한 보안평가 방법론으로는 안전 분야에서 적용하는 위험성 평가 방법을 채택하기로 하였으며 위험성 평가 방법을 요약하면 다음과 같다.

첫째, 운영 중인 시스템이나 수행 중인 작업에 대한 전개

위험성 평가를 하기로 결정된 대상을 정확히 파악하기 위하여 현재 수행하고 있는 업무의 목적, 업무 수행 방법, 적용되고 있는 강제 규정이나 기준, 작성된 업무 표준, 사용하고 있는 장비, 설비, 기기 및 소프트웨어 등을 모두 파악한다. 그리고 현재 시행 중에 있는 안전장치에 대해서도 파악하여야 한다.

둘째, 위험 파악

운영 중인 시스템이나 수행 중인 작업에 내재되어 있는 위험을 찾아내기 위하여 위험 파악을 시행한다. 위험 파악 단계에서는 숨어있는 위험 요소를 모두 찾아내야 하며 그 위험 요소들이 가지고 있는 특성을 정확히 규명해야 한다. 위험 파악을 위해서는 많은 분야의 사람들이 참석하는 것이 필요하다. 일부 몇 사람만 참여하여 위험 파악을 수행하면 제한된 시각의 위험만 식별이 될 수 있다. 그러므로 내재되어 있는 위험을 누락시키지 않고 식별하기 위해서는 위험성 평가 대상과 관계되는 모든 분야를 대표하는 사람들이 참석하여 위험 파악을 진행하여야 한다.

위험 파악을 할 때는 두 가지 기본적인 접근 방법이 있다. 먼저 이미 축적된 경험과 근거 규정을 활용하는 것과, 경험이 축적되어 있지 않은 경우 적용하는 예측 위험 요소 파악 방법이다.

파악된 위험에 대해서는 그 위험이 발생할 수 있는 원인들을 면밀히 검토하여 식별한다.

셋째, 발생 결과 평가

파악된 위험이 사고로 진전되었을 경우에 나타나는 결과에 대하여 평가한다. 한 가지 이상의 결과가 나올 수 있으며 이 경우 예상되는 모든 결과를 파악하여야 한다.

넷째, 빈도/가능성 평가

파악된 위험이 사고로 진전될 수 있는 빈도나 가능성을 평가한다. 빈도/가능성을 평가할 때는 현재 수행 중에 있는 업무 절차, 적용하고 있는 기준 그리고 현재 적용되고 있는 안전조치를 고려하여 판단하여야 한다.

다섯째, 위험성 산정 및 등급 결정

예상되는 결과와 빈도/가능성을 근거로 위험서의 크기를 확정하고 등급을 산정한다. 위험성의 크기를 확정하고 등급을 산정하는 방법은 행렬 매트릭스를 사용하여 구하는 것이다. 발생 결과 평가에서 구한 것과 빈도/가능성 평가에서 구한 것을 각 각 등급으로 분류한 후 이 두 가지 등급을 가지고 행렬 매트릭스를 구성한다.

여섯째, 개선대책 수립

위험성 등급이 높은 것으로 결정된 사항에 대하여는 위험성 등급을 낮출 수 있는 대책을 수립하여야 한다. 개선대책을 수립할 때는 위험을 발생시키는 원인을 근본적으로 제거하는 방법을 가장 먼저 고려하여야 하며, 원인을 근본적으로 제거하는 것이 불가능 할 경우에는 위험이 사고로 진전되지 않도록 적절히 관리하기 위한 방법을 다음으로 고려하여야 하고, 위험이 진전되어 사고가 발생하였을 때 피해를 최소화 할 수 있는 방법을 마지막으로 고려하여야 한다.

개선대책은 심각성을 낮추는 것보다 빈도/가능성을 줄이는 방법을 먼저 고려하는 것이 바람직하다. 또한 비용 효과 측면을 고려하여야 한다. 그리고 개선대책이 기술적인 향상을 필요로 하는 경우에는 현재 기술로서 달성 가능한 정도인지 아닌지를 판단하여야 한다.

일곱째, 개선대책에 대한 위험성 재평가

적용 가능한 개선대책을 수립한 경우에는 개선대책을 실행에 옮기기 전에 이 개선대책이 실제적으로 위험성 등급을 낮추는지를 확인하여야 한다. 재평가는 발생 결과 평가 단계부터 다시 평가를 진행하여 위험성 등급을 확인하여야 한다.

위험성 평가 방법을 모델로 전개한 항만시설 보안평가 방법은 다음과 같다.

1단계, 보호해야 할 주요대상 식별 및 우선순위 평가

항만시설 내의 시설물이나 기반시설의 기능을 명확하게 식별하여 보안위협이나 보안사건으로부터 보호하기 위한 시설물이나 기반시설을 식별한다. 보호해야 할 대상으로 식별된 시설물이나 기반시설에 대하여는 상대적 중요성에

대한 우선순위를 평가하여 항만시설 보안평가를 수행하기 위한 대상을 결정한다.

우선순위는 시설물이나 기반시설이 가지고 있는 기능이나 임무, 시설물이나 기반시설이 손상 또는 파괴되는 경우에 미치는 영향, 시설물이나 기반시설이 손상 또는 파괴되는 경우에 항만시설 운영에 미치는 영향 및 복구 능력 등을 기준으로 하여 평가한다.

2단계, 현장보안상태 확인

현장보안상태 확인은 다음 세 가지 목적을 달성하기 위하여 시행한다.

첫째, 항만시설 또는 항만시설 내의 시설물이나 기반시설에 대한 현재의 보안상태를 파악한다.

둘째, 향후 완화조치를 시행할 경우 완화조치 방법을 결정하기 위한 근거를 제공한다.

셋째, 현재의 보안상태를 각 평가 항목별 기준에 따라 평가하여 보안수준을 확인한다.

3단계, 위협 시나리오 및 보안사건 식별

항만시설의 주요 대상에 내재되어 있는 보안위험요소를 식별하기 위하여 보호해야 할 필요가 있다고 식별된 주요 대상에 대하여 위협을 줄 수 있는 보안위협과, 식별된 보안위협이 사건으로 전개될 때 발생할 수 있는 보안사건에 대한 시나리오를 식별한다.

보안 위협 시나리오 및 보안사건을 식별할 때는 과거에 발생했던 보안사건, 보안관계기관과의 협의 또는 자문, 이미 제정되어 있는 보안관련 강제 규정을 고려하여야 한다.

4단계, 심각성 및 취약성 평가

식별된 보안사건이 발생된 경우 미치는 영향 및 발생할 수 있는 가능성을 확인하기 위하여 심각성 및 취약성을 평가한다. 심각성은 보안사건이 발생되었을 때 입을 수 있는 인적 손상, 재산적 피해, 국가적 영향 등으로 구분하여 평가하며, 취약성은 접근용이성과 보안조직성 두 부분을 구분하여 평가한다. 또한 취약성을 평가할 때는 현재 시행되고 있는 보안시스템을 감안하여 평가한다.

5단계, 보안위험성 평가

심각성과 취약성 등급을 기준으로 위험성 등급을 산정한다. 위험성은 현재 조치유지, 완화조치검토, 완화조치필요의 3등급으로 구분한다.

6단계, 완화조치 대상 선정 및 완화조치 방법 결정

보안위험성 등급을 평가한 결과를 바탕으로 완화조치를 해야 할 필요성이 있는 부분을 식별하고, 완화조치가 필요한 부분에 대하여는 적절한 완화조치가 어떤 것인지 식별한다.

완화조치 방법을 결정할 때는 효과성과 실행 가능성을 복합적으로 평가하여 결정한다. 또한 심각성 등급을 낮추는 방법보다 취약성 등급을 낮추는 방법을 먼저 고려하는 것이 필요하다.

7단계, 보안위험성 재평가 및 완화조치 확정

완화조치를 하기로 결정한 완화조치 방법에 대하여 실제 보안위험성 등급이 낮아지는지 확인을 한다. 심각성 및 취약성 평가 단계에서 다시 평가를 시행하여 원하는 수준으로 보안위험성 등급이 완화되는지 확인한다. 재평가 결과 보안위험성 등급이 완화되지 않으면 완화조치로 채택하지 않고 추가의 완화조치를 고려하여야 한다. 재평가 결과 보안위험성 등급이 허용되는 수준까지 완화되는 경우에는 이 완화조치를 채택하고 항만시설보안시스템에 반영하기 위한 계획을 수립하여야 한다.

제2절 연구결과의 시사점

본 연구결과의 시사점은 다음과 같다.

먼저 항만시설의 보안시스템을 수립하기 위하여 필수적으로 선행되어야 하는 보안평가를 시행하기 위해서는 체계적인 접근이 필요하다. 이를 위해서는 우선 ISPS Code에 대한 이해가 필수적으로 필요하디. ISPS Code에서 요구하고 있는 항만시설 보안평가 요구사항을 정확히 인식하고 보안평가를 통해서 확인해야 할 사항이 무엇인지 명확히 파악을 하고 보안평가를 시행하여야 한다. 특히 ISPS Coda B편에 제시되어 있는 지침을 어떻게 수용하여 적용할 것인지를 면밀히 검토하여야 한다. 항만시설의 입장에서는 ISPS Code B편에 있는 내용이 강제적으로 적용되는 부분은 아니지만 실질적으로 B편에 있는 지침을 무시하고 보안평가 및 보안시스템을 수립하기란 현실적으로 불가능하다고 할 수 있다. 결국 항만시설도 B편의 지침을 반영하여야 ISPS Code에 적합한 보안시스템을 수립할 수 있다. 그러므로 항만시설의 보안평가를 수행하는 자는 ISPS Code의 내용을 충분히 파악하고 있어야 한다. 이를 위해서는 전문 교육기관의 교육을 필수적으로 이수하여야 할 것이다.

다음은 보안평가 방법론에 관한 부분이다.

보안평가를 효과적이고 효율적으로 진행하고 위험성 등급이 높은 부분에 대한 실행 가능한 대응조치를 마련하기 위해서는 논리적으로 명확한 체계를 가지고 있는 보안평가 방법론이 필요하다. 여러 가지 다양한 보안평가 방법론이 있을 수 있으나 안전 분야에서 적용하고 있는 위험성 평가 방법을 모델로 보안평가를 시행하는 것이 가장 적절하다고 판단된다.

다음은 보안평가 시행에 관한 부분이다. 보안평가를 수행하기 위해서는 현장보안상태 확인 및 다양한 데이터의 수집이 필요하다. 비록 보안평가가 정량적인 평가방법은 아니라도 데이터를 가지고 체계적으로 평가를 하므로 적절한 데이터가 반영되지 않으면 나타나는 결과가 올바르지 않을 수 있다. 그리고 보안평가를 수행하는 자는 위험성 평가 방법에 대한 개념을 충분히 인지하고 있어야 할 것이다.

제3절 연구의 한계와 향후과제

본 연구는 ISPS Code에 따른 항만시설 보안평가를 시행하기 위한 방법론을 제시함으로써 항만시설 운영자들이 보안시스템을 수립하기 위한 선행 과정으로서 보안평가를 시행하는데 다소 기여를 할 수 있다고 생각한다. 그러나 ISPS Code가 시행 된지 얼마 되지 않아서 선행 연구 자료를 많이 접할 수 없음으로 인하여 연구를 진행하는데 어려움을 겪을 수밖에 없었다. 이런 점을 감안할 때 다음과 같이 본 연구의 한계와 이를 극복하기 위한 향후 연구방향을 제시한다.

첫째, 심각성과 취약성을 평가하는 기준을 설정함에 있어서 구체적인 수치로서 제시되지 못한 부분이 있었다. 국가적인 기준이나 통념적으로 적용되는 기준이 없음으로 인하여 정성적인 사항으로서만 제시가 되었기 때문에 평가에 다소 혼란과 오차가 있을 수 있을 것이다. 향후의 연구에서는 이 부분에 대한 연구가 활발하게 진행되어 우리나라 항만의 실정에 맞는 기준이 제시되는 것이 필요하다고 생각한다.

둘째, 보안위협 정도는 외부의 상황이 어떻게 변화하느냐에 따라 전적으로 영향을 받는다고 볼 수 있다. 변화하는 보안위협이 보안 취약성에 어떻게 영향을 미치는지 그리고 보안평가를 할 때 어떻게 반영되어야 하는지가 명확하지 못한 부분이 있었다. 향후에는 보안위협의 정도가 보안위험성 등급을 결정하

는데 어떤 영향을 미치는지에 대한 연구가 필요하다고 생각한다.

셋째, 본 연구는 원칙적인 방법론에 대하여만 제시가 되었기 때문에 기존의 보안관련 국내법과의 관련 여부를 파악하지 못한 부분이 있다. 향후에는 ISPS Code에 따른 항만시설의 보안평가를 시행하는 것이 국내법에서는 어떻게 수용되어야 하는 지에 대하여 활발한 연구가 진행되었으면 한다.

참고문헌

국내문헌

1. 김영호, 고재욱, 김동환. 임동호, 윤석준 편저, 「안전보건경영실무」, 대영사, 2000
2. 안영진, 「21세기 기업경쟁력 강화를 위한 TQM:품질경영」, 박영사, 2000
3. 주종대, 조지훈, 「위험과 운전분석」, 한국산업안전공단, 2001
4. 한국산업안전공단, "안전보건경영시스템 구축에 관한 지침(KOSHA Code G-04-2003)", 2003
5. 한국선급, 「ISPS Code CSO/SSO Training Course」, 2003
6. 한국선급, 국제 선박 및 항만시설 보안규칙, 2003
7. 한국인정원, "K-OHSMS 18001 안전보건경영시스템 - 요구사항", 2001

국외문헌

1. ISPS Code Part A / Part B
2. USCG Maritime Transportation Security Act(MTSA) of 2002
3. USCG 33 CFR Subchapter H
4. USCG NVIC 04-02 : Security for passenger vessels and passenger terminals, 2002. 3. 29.
5. USCG NVIC 9-02 : Guidelines for port security committees, and port security plans required for U.S. ports, 2002. 9. 30.
6. USCG NVIC 9-02(Change 1) : Guidelines for development of area maritime security committees and area maritime security plans requires for U.S. ports, 2003. 12. 15.
7. USCG NVIC 10-02 : Security guidelines for vessels, 2002. 10. 21
8. USCG NVIC 10-02(Change 1) : Security guidelines for vessels, 2004. 8. 6.
9. USCG NVIC 11-02 : Recommended security guidelines for facilities, 2003. 1. 23.
10. USCG NVIC 11-02(Change) : Recommended security guidelines for facilities, 2004. 8. 6.
11. USCG NVIC 03-03(Change 1) : Implementation guidance for the regulations mandated by the maritime transportation security act of

2002(MTSA) for facilities, 2004. 5. 27.
12. USCG NVIC 04-03(Change 1) : Implementation guidance for the regulations mandated by the maritime transportation security act of 2002(MTSA) for facilities, 2004. 5. 21.
13. USCG NVIC 05-03 : Implementation guidance for the maritime security regulations mandated by the maritime transportation security act of 2002(MTSA) for outer continental shelf facilities, 2003. 12. 15.
14. USCG NVIC 06-04 : Voluntary screening guidance for owners or operators regulated under parts 104, 105, and 106 of subchapter H of title 33, code of federal regulations, 2004. 5. 27.
15. IMO/ILO Code of practice on security in ports, 2003. 12. 24.
16. USCG Port Facility Survey Program(Draft), 2004
17. ISO/PAS 20858 : 2004(E) Ships and marine technology-Maritime port facility security assessments and security plan development, 2004