

1. ISPS Code에 규정된 항만시설 보안평가를 시행하기 위한 방법론에 관한 연구

해운경영학과 김 영 균
지도교수 김 길 수

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.

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(1974 SOLAS, 이하 SOLAS라고 함)에 제11-2장 해상보안 강화를 위한 특별조치를 신설하였다. 또한 선박 및 항만시설(port facility)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 규칙으로 ISPS Code를 시행하도록 하는 근거 규정을 마련하였다.

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.

항만시설이 효과적이고 적절한 보안시스템을 수립하기 위해서는 체계적인 접근이 필요하다.

본 연구에서는 항만시설이 ISPS Code에서 요구하는 보안시스템을 제대로 수립하기 위해

서는 보안시스템 수립에 선행하여 시행하는 보안평가를 정확히 실시하여야 하며 보안평가를 정확히 실시하기 위해서는 보안평가를 하는데 적절한 방법론이 필요하다는 것을 알 수 있었다. 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.

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 보안위험이나 보안사건으로부터 보호하기 위한 시설물이나 기반시설을 식별한다. 보호해야 할 대상으로 식별된 시설물이나 기반시설에 대하여는 상대적 중요성에 대한 우선순위를 평가하여 항만시설 보안평가를 수행하기 위한 대상을 결정한다.

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 보안위험과, 식별된 보안위험이 사건으로 전개될 때 발생할 수 있는 보안사건에 대한 시나리오를 식별한다.

4단계, 심각성 및 취약성 평가

식별된 보안사건이 발생된 경우 미치는 영향 및 발생할 수 있는 가능성을 확인하기 위하여 심각성 및 취약성을 평가한다.

5단계, 보안위험성 평가

심각성과 취약성 등급을 기준으로 위험성 등급을 산정한다. 위험성은 현재조치유지, 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.

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 완화

조치로 채택하지 않고 추가의 완화조치를 고려하여야 한다. 재평가 결과 보안위협성 등급이 허용되는 수준까지 완화되는 경우에는 이 완화조치를 채택하고 항만시설보안시스템에 반영하기 위한 계획을 수립하여야 한다.

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 필요하다. 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 위협성 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 위협성 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 결과에 올바르게 않을 수 있다. 그리고 보안평가를 수행하는 자는 위협성 평가 방법에 대한 개념을 충분히 인지하고 있어야 할 것이다.

2. 남북중단철도(TKR)와 시베리아횡단철도(TSR)의 연결이 우리나라 국제운송물류시장에 미치는 영향에 관한 연구

- TSR을 중심으로 -

해운경영학과 고 승 우
지도교수 신 한 원

세계시장이 외국무역의 급성장과 함께 글로벌화 되어짐에 따라 극동 경제망의 역할이 어느 때보다 중요시되고 있다. 현재 러시아를 포함한 유럽지역, 중앙아시아 지역과 교역·경제협력의 확장 또한 가속화되고 있다. 우리나라가 동북아 물류중심지로 자리 잡기 위해서는 해운과 항공부문뿐만 아니라, 철도를 이용한 육상운송부문의 육성도 필요하다. 따라서 국내