論 文

고위험 테러시대 선박보안시스템 구축을 위한 기초 연구

이 은 방*

A Basic Study on Development of Merchant Ship's Security System in High-Risk Terrorism

Eun Bang LEE

〈目 次〉

Abstract
1. 서론
2. 선박 보안관리의 특성
2.1 해양의 보안환경 및 취약성
2.2 선박보안관리의 원칙
2.3 선박보안위험 종류
3. 선박 보안위험 관리
3.1 보안위험 평가
3.2 Ship Security Risk Management
3.3 위험 평가와 의사결정 시스템
4. 선박의 보안 모델
4.1. 인적 보안시스템
4.2. 해양 및 선박 보안 시스템
5. 결론
참고문헌

Abstract

With the terrorist attacks on 11 September 2001, the ships and their crews' safety and security have become a major issue in the maritime industries. In high-risk terrorism, not only ship owners and port authorities but also crewmembers on board should take precautions in the conduct of their business. In this paper, the vulnerability and essential elements in overall security of merchant ship are analyzed with a discussion in depth of the concept and principles of maritime security management. Author proposes ship's security model to reduce security risk and to minimize damage as a basic study for designing security system for merchant ship.

제1장 서 론

인류가 해상활동을 시작한 이래로 해양에서의 물적, 인적재해를 예방하기 위한 교육 및 훈련, 안전장비의 개발, 안전관련 법안의 입안과 집행 등의 노력에 힘입어 해난사고는 꾸준히 감소하는 추세이다. 선박에 의한 해상활동은 광활성, 고립성, 고위험 특성을 가진 행위로 선박, 인명, 환경에 대한 안전의 담보가 요구되어 왔다. 초기에는 선박운항자의 경험과 자질에 의존하였기 때문에 소화, 퇴선, 인명생존에 대한 교육과 훈련 등 주로 개별선박의 자력에 의한 안전확보 방안이 강구되어졌다. 점차로 과학기술의 발달로 신뢰성이 향상된 안전장비가 개발되어 해난의 위험을 낮출 수 있었으며, 전파와 위성을 이용한 통신기술의 발달로 선박 간의 협조는 물론 육상의 지원이 가능해져 해상의 안전도는 크게

* 한국해양대학교 해양경찰학과 교수
eunbang@hhu.ac.kr

높아졌다. 해상안전에 대한 국제적인 관심도 높아져SOLAS를 비롯한 국제협약이 체결되었고 ISM(International Safety Management) code의 도입으로 해상활동의 안전문화가 정착되어 가고 있다.

그러나 2001년 9월 11일 뉴욕과 워싱턴에서 발생한 항공기를 이용한 테러사건 이후로 해양산업에 있어서 해양안전(maritime safety)에 부가해서 보안(security)의 대책이 요구되고 있다. 국제사회는 신속하게 해양보안대책으로 ISPS(International Ship and Port facility Security)code제정하여 테러를 예방하고 퇴치함은 물론 해상에서 보안을 강화하기 노력을 계속하고 있다[1]. 미국의 테러사건 이전에는 선박에서의 보안확보 노력이 주로 도난, 밀수, 마약의 예방에 초점이 맞추어 졌으나 앞으로는 테러, 화학무기를 비롯한 대량 살상무기의 방지까지 확대되고 있다. 이와 같은 고위험 테러시대에 선주와 항만 당국은 물론 선박의 현장 종사자들도 선박테러에 대한 경각심과 대비책이 강구되어야 한다.

본 연구에서는 선박 보안을 위한 필수적인 요소와 취약성을 분석하고 상선보안관리의 개념 및 원칙을 살펴보았다. 또한 상선의 보안시스템 구축을 위한 기초연구로써 보안위험을 줄이고 재해를 최소화 할 수 있는 선박의 보안 모델을 제시하고자 한다.

2. 선박 보안관리의 특성

2.1 해양의 보안환경 및 취약성

해양은 세계 물동량의 90%이상을 운반하는 교통로 이용될 뿐만 아니라, 해저자원과 수산자원의 생산 공간으로, 해양스포츠 및 관광의 문화공간으로 그 이용이 날로 증가되고 있다. 국제적으로 해양이용권의 주도권과 해양영토 확장의 경쟁이 날로 심화되고 있으며 유엔해양법협약 발효와 주요 연안국들의 배타적경제수역 선포 등 본격적인 해양분할시대로 접어들고 있다. 한반도 주변해역에서도 수산자원과 해저자원의 보호문제, 해양환경보존 문제는 물론 마약 및 불법무기의 유통문제 등 해양보안환경이 급변하고 있다. 또한 미국의 테러사건 이후로 사적인 이욕을 위해 저질러지는 해적행위뿐만 아니라 정치적 목적을 가진 집단의 테러행위에 대한 대비와 경계가 요구되고 있다.

해양을 항로로 이용하는 상선은 선박의 자체 재산가치와 탑승자의 인명에 대한 위협, 환경과 경제의 간접재해의 광대성으로 장시간 언론의 관심이 집중될 수 있기 때문에 테러 수단으로 이용될 개연성이 높다[2]. 선박의 테러에 대한 취약성으로는 첫째, 광활한 해양을 항로로 이용하기 때문에 교통의 통제 및 제어가 어렵다. 둘째, 해안의 인구 밀집 대도시의 접근이 용이하다. 셋째, 대량의 화물 운송으로 위험물질의 검사가 어렵고 육상 교통수단과 연계로 확산이 쉽게 이루어 진다. 넷째, 상선에는 특별한 자체 보안장비가 설치 되어 있지 않다. 다섯째, 테러 분자들이 선박 접근이 용이하다. 여섯째, 선박의 규모에 비하여 테러 대응 인원이 소수이다. 일곱째, 테러 억지세력의 지원이 어렵다.

2.2 선박보안관리의 원칙

2.2.1 선원 및 선박운항관련자에 대한 관련자의 보안 경각심 고취

〈표1〉과 같이 회사보안사관(Company Security Officer: CSO), 선박보안사관(Ship Security Officer: SSO), 승무원에 대하여 필요한 선박보안교육, 훈련 및 실습을 통한 보안지식 및 능력을 배양한다.

〈표1〉 보안교육, 훈련 및 실습내용

분 류	내 용
보안행정	국제관련협약 및 법률
검사기술	검사, 통제, 검사기법
	반입물건의 검색방법
	위험물질, 위험장치 식별
보안 기술	보안위협 인지법
	군중 통제기법
	보안조치 기법
	비상절차 및 계획
	선박의 보안검사
보안 장비	보안장비의 유지관리
	보안장비 및 시스템 운용
	보안통신장비 운용
기타	보안관련 정보 취급
	보안위협과 유형에 관한 지식

2.2.2 테러위험을 방지하기 위한 보안능력 강화

보안등급(Security level)에 따라 〈표2〉와 같은 내용의 선박보안계획서(Ship Security Plan)를 수립이 필요하다.

〈표2〉 보안계획서의 내용

구분	내 용
1	선박의 상세 보안조직 구성
2	선박보안책임에 대한 선박회사, 항만당국, 타선박과 관계설정
3	항만당국, 선박간 지속적인 통신시스템 운용
4	보안등급 1,2,3에서 기본 보안대책
5	관련당국과의 보고 절차

2.2.3 선내 주요시설의 보호

〈표3〉 의 선내 장소 및 시설에 권한을 가진 사람들만의 접근을 확인하기 위한 모니터링이 필요하다.

〈표3〉 선내 제한구역

구분	장소 및 시설
1	선교(Navigational bridge)
2	중앙제어장소(Control stations and central control station)
3	주요 기계설비Machinery space(main engine, generator, steering gear....)
4	물탱크, 펌프, manifold와 연결 장소
5	화물 펌프실
6	기타(선박보안 필요한 장소)

2.2.4 테러 억제 및 대응 능력의 강화

(1) 선박이 보안에 위협에 직면한 경우에 가까운 연안국 및 치안세력에게 도움을 요청하기 위한 〈표4〉 와 같은 요건을 가진 선박보안경보시스템(ship Alert System)의 설치가 필요하다.

〈표4〉 선박보안시스템의 요건

구분	요 건
1	주관청이 지정한 책임당국에 보안경보를 송신
2	선상에 경보의 송신 무인식(무 알람)
3	다른 선박에 경보신호 무 전송
4	인위적인 재설정 할 때까지 지속적인 보안경보신호 발생

(2) 선박식별번호(Ship Identification Number)를 영구적으로 표시한다.
(3) 보안정보를 국제적으로 통합 관리한다.
(4) 테러억지 지원세력(해군, 해경) 협력체제를 구축한다.

2.2.5 고위험 수역에서 능동적 선박 운항 제어

(1) 선박자동식별시스템(Automatic Identification System: AIS)조기 도입을 통한 선박의 위치 추적을 한다.
(2) 선박이력기록부(Continuous Synopsis Record: SCR) 도입하여 선박의 정보를 관리한다.
(3) 회사보안검사관(CSO)이 전 자사선박의 보안관리를 일원화하고 그 에 대한 권한과 책임 부여한다.

2.3 선박보안위험 종류

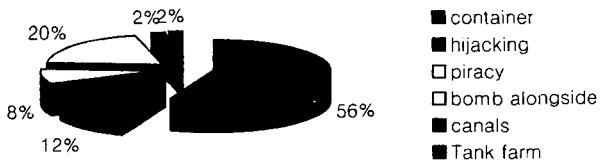
선박의 잠재적인 보안위협 종류는 다음과 같다[3] [4].

(1) 테러 : 선박을 자체무기로 이용하여 육상의 타 시설을 공격하거나 화학무기를 비롯한 대량테러 무기의 수송수단으로 이용이 가능
(2) 무장해적: 여러 지역(항만, 협수로, 연안항해)에서 상선에 심각한 보안위협
(3) 마약유통: 마약의 생산지로부터 마약의 운반 및 판매
(4) 무기유통: 총기류, 폭발물, 생화학무기를 비롯한 대량 살생무기의 운반 및 유통
(5) 밀항:적합한 출입국 절차 없이 선박을 통하여 해외로 이동행위
(6) 납치:승무원의 안전 위협대가로 정치적, 금전적 대가 요구행위
(7) 파괴행위(vandalism): 특정 목적 혹은 요구불만 등의 정신 불안으로 선박의 파괴나 침몰행위
(8) 노동자의 단체행동:항만의 노동자의 노조 및 그룹의 투쟁
(9) 승무원의 폭력 및 폭동: 우발적인 감정의 대립으로 인한 개인적인 폭력행위 또는 요구불만에 대한 집단적인 폭력에 의한 집단행동

〈그림 1〉은 해양산업별 테러리스트에 의한 위협 가능성에 대한 조사 내용이다. Connecticut해운회사조합(CMS) 의한 업계 관계자에 대한 설문조사에 따르면 container 화물은 운송량의 증가와 더불어 검사의 어려움 등으로 테러위협에 가장 크게 노출되는 것으로 인식되고 있으며 항만에서의 선박 폭파위협이 그 다음으로 나타나고 있다[5].

해상에서의 납치 및 해적사건은 계속 증가하고 있으며 2001년에 21명의 승무원이 살해되고 210명이 인질 사건에 연루되었다. 해상보안사건에 무기의 사용이 현저히 늘어나고 있고 인도네시아 해역, Malacca해역, 아프리카 서쪽해역, 남아메리카 해역이 위험성이 높은 것으로 보고되고 있다[6]. 밀항도 심각한 해상보안위험으로 등장하고 있는 실정이다.

Terrorist threat tomaritime industry(CMS 자료)



3. 선박 보안위험 관리 (Security Risk Management)

3.1 보안위험 평가

보안 평가는 보안위험을 줄이기 위하여 보안위협에 대한 보안 위험을 평가하고 보안조치를 결정하는 과정이다. 일반적으로 보안위험(Security Risk: R)은

보안사고의 가능성(Frequency: F)과 사고에 의한 피해의 심각성(Consequence: C)의 두 변수로 다음 식과 같이 표현할 수 있다[7].

$$R = F * C \quad (1)$$

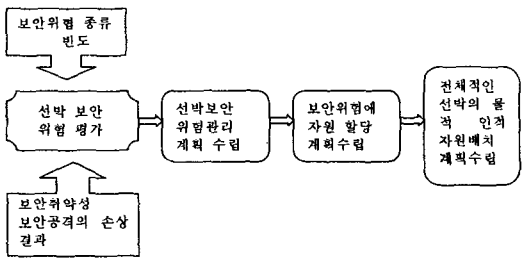
피해 심각성(C)은 보안위협으로 인한 공격에 의하여 발생하는 인적, 물적, 환경적 손실과 이에 부가되는 간접 손실의 합으로 표현된다. 발생 가능성(F)는 어떤 목표물 혹은 시나리오에 대하여 특정한 형태의 보안공격의 발생 정도인 보안 위협(Threat: T)과 이들 위협에 대한 실패 가능성 정도인 보안 취약성(Vulnerability: V)으로 다음 식과 같이 표현할 수 있다.

$$F = T * V \quad (2)$$

따라서 R=T*C*V로 표현된다.

3.2 Ship Security Risk Management

보안업무에 대한 책임은 보안공격에 대한 억지세력을 보유한 군대 혹은 경찰에 있는 것으로 인식되어 보안위험에 대한 사고결과의 심각성에 비하여 다른 형태의 위험(Risk)과는 달리 최근까지 큰 관심을 받지 못하여왔다. 선박에 대한 테러와 같은 보안공격은 자연재해위험, 안전사고위험, 재정위험 등과는 다른 형태의 위협이지만 같은 방법으로 위험을 효과적으로 관리하기 위한 〈그림 2〉는 Ship Security Risk Management System를 도입할 수 있다.



〈그림 2〉 선박 보안위험관리 시스템 개념도

3.3 위험 평가와 의사결정 시스템

해상에서 선박이 직면할 선박 보안 사건에 대하여 올바른 보안위험 평가를 바탕으로 유효하고, 실현 가능한 효과적인 의사결정을 하기 위하여서는 적절한 정보수집방법과 구조화된 의사결정 시스템이 필요하다. 〈그림 3〉 위험기반 의사결정시스템의 개념도이다.

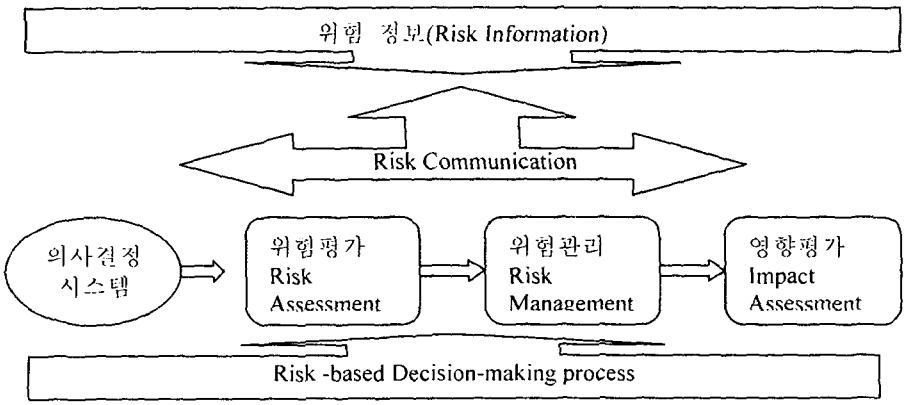
위험기반의사 결정은 다음 순서로 이루어질 수 있다. 첫째, 의사결정 시스템을 구조화한다. 둘째, 다양한 방법으로 위험에 관한 정보를 수집하여 위험을 인지한다. 셋째, 위험 평가기법을 바탕으로 한 프로그램을 통한 위험을 평가한다. 넷째, 위험회피, 위험제거, 위험분산 등으로 위험을 제어 관리한다. 다섯째, 위험관리의 결과를 평가함으로써 각 단계별 개선방법을 강구한다.

4. 선박의 보안 모델

4.1 인적 보안시스템

4.1.1 선박의 보안조직

선박이 자동화됨으로써 급격하게 승무원 수의 감소와 더불어 다국적 선원이 함께 승선하는 선박의 수가 날로 늘어나고 있다. 승무원수의 감소는 선박의 안전운항 뿐만 아니라 보안위험을 증대 시키어 위험을 인지하고 예방, 대응책을 수립하는데 많은 어려움을 주고 있다. 한편 다양한 문화와 습관을 가진 다국적 선원이 함께 승선함으로써 승무원간의



〈그림 3〉 위험 기반 의사결정 과정

갈등에 의한 폭력 및 폭동의 직접적인 잠재보안 위험이 높아지고 있다.

보안에 잠재적인 취약성을 극복하기 위해서는 선박의 특성, 승무원수, 선박의 상황, 항로, 기항지의 상황 등을 고려한 선박의 보안조직이 필요하다. 〈표 5〉는 승무원의 보안업무의 분담의 예를 나타낸다. 보안위험을 줄이기 위한 예방조치는 물론 보안공격 대비한 체계적인 대응조치가 강구되어야 한다.

〈표5〉 보안조직과 임무

구분	직책	임 무	기타
1	선장	선박안전 · 보안 총괄 지휘	
2	C/O	선박보안계획수립 및 집행	보안사관
3	2/O	선교 보안 및 보안서류적성 관리	
4	3/O	선장보좌, 구명정 및 의약품 보안	
5	기관장	기관실 보안 책임	
6	1/E	선내 기관 추진력 및 전원보안	
7	2/E	기관실내 유류 및 고압탱크 보안	
8	3/E	기관 제어실 보안	
9	R/O	통신실 보안책임, 보안경보시스템 보수유지	
10	갑판장	화물 통제실 보안책임 및 선내 창고 보안	
11	AB1	출입보안시스템 관리	
12	AB2	출입보안시스템 관리	경보시스템
13	AB3	2/O보좌 및 선교 출입관리	
14	조기장	기관실 출입보안시스템 관리	
15	O1	1/E 보좌, 주기 및 발전기 담당	경보시스템
16	O2	기관실 창고 보안 담당	
17	O3	2/E보좌 및 조타실 담당	
18	사주장	조리실 및 식량, 식수 보안	
19	C1	음식물 보관창고 보안	

4.1.2 Prevention Through Crew Program (PTC)

일반적으로 상선은 보안공격에 대해서 자기방어를 위한 무기체계를 가지고 있지 않다. 또한 항구이외에서 외부의 보안세력지원을 받기에도 많은 시간이 필요할 뿐만 아니라 고압가스, 유류, 위험화물 등 테러 단체들이 테러 무기화 할 수 있는 많은 물질과 설비를 가지고 있다. 또한 승무원도 해적과 같은 단순한 보안 공격을 제외하고는 상선의 보안 취약성을 인식하고 있지 않고 보안에 대한 교육, 훈련의 부족으로 보안대응능력도 낮은 실정이다.

광활한 대양을 고립성을 가지고 운항되는 상선의 보안위험을 낮추기 위해서는 무엇보다도 승무원의 의한 테러대응 프로그램 구축이 필요하다. 〈표 6〉은 승무원에 의한 테러대응 PTC 프로그램을 나타낸다[8].

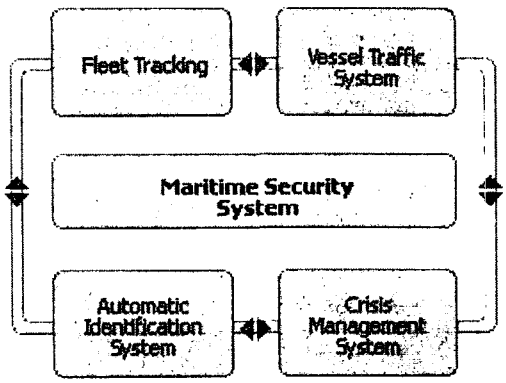
〈표6〉 Prevent Through Crew program

구분	목 표	내 용
1	Know More	선박의 보안 위험의 종류, 취약성
		테러대응기술, 보안위험관리법 등
2	Train More	테러대응훈련, 보안장비사용법, 보안검사법
		위험물 취급 및 식별법, 무기류 사용법 등
3	Caution More	항로의 위험요소, 출입자, 항만 사정
		적재화물의 위험성, 보안정보 등
4	Offer More	위험정보, 상선의 보안장비, 보안조치
		보안계획의 개선책 등
5	Cooperate More	보안지원세력과 협조 체제, 국제적 협조체제
		선박, 항만당국, 연안국 협조체제 등

4.2 해양 및 선박 보안 시스템

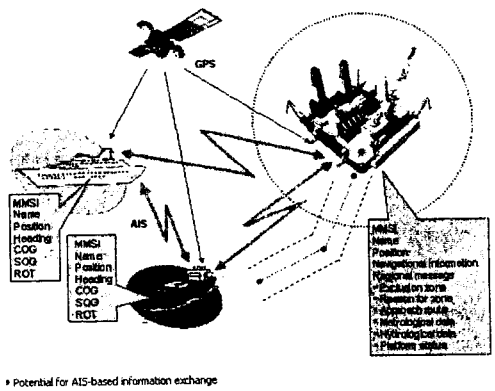
4..2.1 해양보안 시스템

〈그림 4〉는 Transa회사 해양보안 시스템의 개념도를 나타낸다. Radar와 위성, AIS 시스템을 이용하여 선박의 정보를 수집하고 그 정보를 바탕으로 최적의 보안위험관리를 수행한다[9].

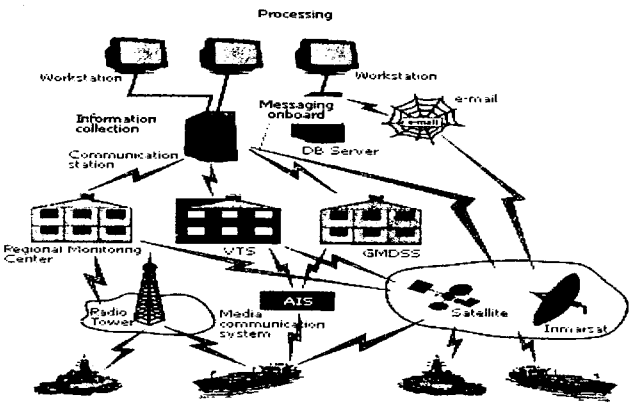


〈그림 4〉 해양보안 시스템의 개념도

〈그림 5〉은 선박의 정보를 수집하기 위한 AIS시스템을 나타내고 〈그림 6〉은 AIS, 통신위성, VTS, 통신시스템을 이용한 선박 모니터링 시스템을 나타낸다.



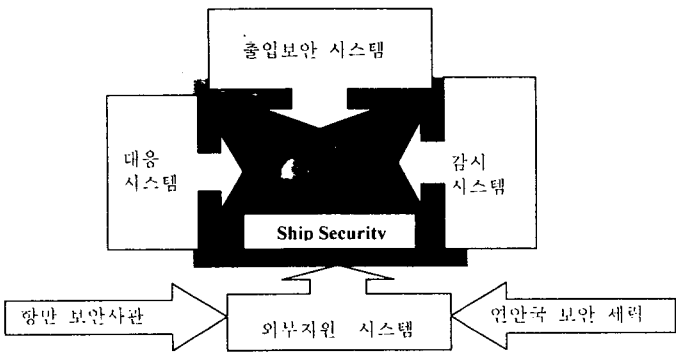
〈그림 5〉 Automatic Identification System



〈그림 6〉 선박 모니터링 시스템

4.2.2 선박 보안시스템

선박의 보안위험을 예방하고 보안 공격을 받았을 때 효과적인 대응체계 수립을 위해서는 선박의 추적 및 모니터링 시스템과 같은 해양보안 시스템과 더불어 개별 선박의 보안 시스템이 필요하다. 선박의 보안 시스템은 출입자의 출입을 통제하는 출입보안 시스템, 선박주위 및 주요 시설물의 감시를 위한 감시 시스템, 보안공격에 의한 피해를 최소화하기 위한 대응 시스템, 외부지원 세력의 지원과 공동 대응을 위한 외부 지원 시스템으로 구성될 수 있다. 〈그림 7〉은 선박보안 시스템 구성도 이다.



〈그림 7〉 선박보안시스템의 구성도

(1) 출입 보안시스템: 출입자 ID확인 장치, 승무원의 ID card, 소지품 검사 시스템 등
(2) 감시 시스템: CCTV, 접근금지 구역 경보 시스템, 위험물 감지 시스템 등
(3) 대응 시스템 : 가스 총, lock system, 수갑 등
(4) 외부 지원시스템 : ship alert system, 비상교통신망 등

5. 결 론

미국의 테러사건 이후 해양산업과 상선에 대한 테러경각심이 높아지고 있다. 자체의 방어 무기체제 없이 광활한 해상을 활동 무대로 하는 상선은 인명, 선박과 화물의 재산, 환경 및 경제에 미치는 직간접 영향의 광대성 때문에 테러의 목표물이나 수단으로 사용될 개연성이 높다. 본 논문에서는 상선에서의 보안사고를 예방하고 보안위협에 대한 효과적으로 대응하기 위여 선박의 보안관리 특성을 분석하고 보안관리 원칙을 도출하였다. 또한 보안위험의 체계적인 관리기법을 고찰하고 상선의 보안시스템 구축을 위한 기초연구로 PTC 프로그램과 선박의 보안 시스템 모델을 제시하였다.

상선의 보안위험을 낮추기 위해서는 선박의 특성을 고려한 보안 시스템 및 보안장비의 개발과 선박 보안문화 정착을 위한 승무원의 교육·훈련 프로그램 개발 필요하다. 또한 항만과 연안해역에서의 보안지원세력의 주체 선정과 협조체제의 구축되어야 할 것이다.

◈ 참 고 문 헌 ◈

[1] International Ship and Port facility Security code (ISPS), IMO, 2002.
[2] 해상테러억제를 위한 로마협약에 관한 고찰, 신의기, 형사정책연구
제9권 제1호(통권 제33호1998 봄호).
[3] The Coast Guard and Maritime security, Bruce B. Stubbs, JFQ, 2000.8.
[4] Navigation and vessel inspection circular No.1002, United States Coast Guard, 2002, 10.21.
[5] Connecticut Maritime Association Maritime Security Survey Result.
[6] ICC Piracy report.
[7] Modeling Security Risk, Vernon H. Guthrie, David A. Walker, ABS Consulting.
[8] Advancing the principle of the prevention through people program, USCG, 1997.
[9] Navi-Guard security System,
http://www.transas.com/products/navi_guard.