海洋環境安全學會誌 第9卷 第1號. pp. 17~23, 2003. 6. 30 (ISSN 1229-3431)
Journal of The Korean Society of Marine Environment & Safety

# 해양보안위협 대응을 위한 선박보안시스템에 관한 연구

이은방

* 한국해양대학교 해양경찰학과 부교수

# A study on Merchant Ship's Security System for the Correspondence of Maritime Security Threats

*Eun Band Lee**

**Department of Maritime Police Science, Korea Maritime University, Busan, 606-791,Korea*

**요 약** : 2001년 9.11테러사건 이후 선박과 승무원의 안전과 보안문제가 해양산업에서 새로운 화제로 대두되고 있다. 고 위험 테러시대에 선박와 항만당국 뿐만 아니라, 선박 종사자들도 그들의 업무와 행동에 있어서 테러위협에 대한 경각심과 대응책이 요구되고 있다. 본 논문에서는 먼저 해양보안관리의 개념과 원칙에 입각하여 상선의 보안 취약성과 주요 요소를 분석하여 상선보안관리원칙을 도출하였다. 그리고 ISPS 규정에 입각하여 선내의 보안조직과 보안업무를 설정하고 승무원의 보안문화 정착을 위한 PTC 프로그램과 선박보안 시스템을 구성하였다.

**핵심용어** : 해양보안위협, 선박보안시스템, 해양보안관리, 보안위험, 해상보안규정

**ABSTRACT** : *With the terrorist attacks on 11 September 2001, the ships and their crew' 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 crew members 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 of merchant ship are analyzed with a discussion in depth of the concept and principles of maritime security management. And then, ship's security model and security system to reduce security rish and to minimize damage are proposed.*

**KEYWORDS** : *Maritime securityu threats, ships's security system, maritime security management, security rish, ISPS code.*

## 1. 서 론

인류가 해상활동을 시작한 이래로 해양에서의 물적, 인적 재해를 예방하기 위한 노력이 계속되어 왔다. 초기에 해상에서 안전 확보는 소화, 퇴선, 인명생존에 대한 교육과 훈련을 통한 선박운항자의 경험과 자질향상에 초점이 맞추어졌다. 점차로 과학 기술의 발달로 신뢰성이 향상된 안전장비가 개발되고 전파와 위성을 이용한 통신기술이 선박에 도입되면서 해상활동의 위험성이 낮아졌고 선박 간의 협조와 육상의 지원도 가능해져 해상의 안전도는 날로 향상되고 있다. 이와 더불어 해양에서의 인명, 재산 보호와 환경을 보존하고 다양해진 해양 이용자의 안전욕구에 부응하기 위한 해양안전정책 집행으로 국내의 해난사고는 꾸준히 감소하고 있는 추세에 있다.[1] 고립성, 고위험성, 광역성, 국제성, 자연현상 의존 특성을 가진 해상교통 활동에 대한 선박, 인명, 환경 안전에 대한 각종 협약도 발효되어 국제적인 공조 체계도 갖추어져 가고 있다. 특히, ISM(International Safety Management) code의 도입으로 해난방지를 위한 안전관리체계와 안전문화가 정착 되어 가고 있다. 그러나 2001년 9월 11일 뉴욕과 워싱턴 에서 발생한 항공기를 이용한 테러사건 이후로 해양산업에 있어서 해양안전(maritime safety) 대책에 부가해서 해양보안(maritime security) 대책이 요구되고 있다.[2]

특히, 항만, 선박, 해양시설의 보안 취약성이 노출되면서 해상테러행위에 대한 국제적인 관심이 높아지고 있다. 무고한 생명을 위협하거나 빼앗고, 기본적인 자유를 침해하며 인간의 존엄성을 손상시키는 해상테러사건으로는 1985년 10월 7일 이집트 연안에서 이탈이라 여객선 아킬레 라우로(Achille Lauro)호 납치된 사건 2002년 10월 12일 예멘에서 발생한 미구축함 Close호 폭탄공격사건, 2002년 10월 6일 프랑스 유조선 M/T Limburg 에 대한 폭발물 공격사건이 발생하였다. 종래의 해적행위, 밀수, 밀항, 마약유통과 같은 단순한 경제적 이익을 목적으로 하는 해양보안위협에서 정치, 종교적인 주장을 내세운 조직적인 테러, 대량 살생무기유통 등 해양에서 보안위험성이 높아지고 있다.[3] 국제사회는 이와 같은 보안위험을 체계적이

* 종신회원, eunbang@hhu.ac.kr, 051)410-4236

고 효율적으로 관리하여 해상에서 테러를 예방하고 퇴치함은 물론 보안 을 강화하기 위하여 ISPS(International Ship and Port facility Security)code제정하여 2004년 7월 1일 발효를 앞두고 있다. 고 테러 위험시대에 선주와 항만 당국은 물론 선박 현장 종사자들도 선박테러에 대한 경각심을 가지고 대비책을 강구하여 나가야 한다.

본 연구에서는 해상에서 선박보안위협에 효과적으로 대응하기 위한 선박보안시스템 구축을 목적으로 선박보안관리의 특성을 고찰하고 선박보안 취약성을 분석하여 상선 보안관리의 개념과 원칙을 설정하고자 한다. 또한 ISPS code를 선박 현장에 적용하여 선박보안위험성을 낮출 수 있는 방안을 모색하고 각 종의 해양보안위협에 효과적으로 대처하기 위한 인적, 물적 보안시스템을 구축하여 상선의 보안모델을 제안하고자 한다.

## 2.선박보안관리의 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 활용이 날로 증가되고 있다. 국제적으로 해양 이용권의 주도권과 해양영토 확장의 경쟁이 날로 심화되고 있으며 유엔해양법협약 발효와 주요 연안국들의 배타적 경제수역 선포 등 본격적인 해양 분할시대로 접어들고 있다.[4] 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. 2003년 4월에 부산에서 발생한 러시아 갱단에 의한 살인사건은 국내의 항만과 해역도 테러의 장소 및 수단이 될 가능성을 보여주고 있다.

특히 해양을 항로로 이용하는 상선은 선박의 자체 재산 가치와 탑승자의 인명에 대한 위협, 환경과 경제의 직·간접재해의 광대성과 더불어 장시간 언론의 관심이 집중될 수 있기 때문에 테러 수단으로 이용될 개연성이 높다.[5] 선박의 보안위협에 대한 취약성으로는 다음을 둘 수 있다. 첫째, 광활한 해양을 항로로 이용하기 때문에 교통의 통제와 제어가 어렵다. 둘째, 해안의 인구 밀집 대도시의 접근이 용이하다. 셋째, 대량의 화물 운송으로 위험물질의 검사가 어렵고 육상 교통수단과 연계로 확산이 쉽게 이루어진다. 넷째, 상선에는 특별한 자체 보안장비가 설치되어 있지 않다. 다섯째, 테러 분자들이 선박 접근이 용이하다. 여섯째, 선박의 규모에 비하여 테러 대응 인원이 소수이다. 일곱째, 육상의 테러 억지세력의 지원이 어렵다.

### 2.2 선박보안관리의 원칙

#### 2.2.1 선박종사자 및 경영자에게 보안 경각심 고취

Table 1과 같이 회사보안사관(Company Security Officer: CSO), 선박보안사관(Ship Security Officer: SSO), 승무원에 대하여 필요한 선박보안교육, 훈련 및 실습을 통한 보안지식 및 능력을 배양해야한다.[2]

Table 1 Contents of security drills, exercises and training

| 분 류 | 내 용 |
|---|---|
| 보안행정 | 국제관련 협약 및 법률 |
| 검사기술 | 검사, 통제, 검사기법 |
| | 반입물건의 검색방법 |
| | 위험물질, 위험장치 식별 |
| 보안 기술 | 보안위협 탐지 법 |
| | 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 테러위험 예방 능력강화

선박보안 위험을 평가하고 보안등급(Security level)에 따라 Table 2와 같이 보안위협에 대응하기 위한 구체적인 선박보안계획서(Ship Security Plan)를 수립하고 집행해야한다.

Table 2 Contents of ship security plan

| 구 분 | 내 용 |
|---|---|
| 1 | 선박의 상세 보안조직 구성 |
| 2 | 선박보안책임에 대한 선박회사, 항만당국, 타선박과 관계설정 |
| 3 | 항만당국, 선박 간 지속적인 통신시스템 운용 |
| 4 | 보안등급별(level 1,2,3) 기본 보안대책 |
| 5 | 관련당국과의 보고 절차 |

2.2.3 선내 주요시설의 통제

Table 3의 선내 장소 및 시설에 권한을 가진 사람들만의 접근을 확인하기 위한 모니터링 시스템을 설치해야 한다.

Table 3 Restricted areas

| 구 분 | 장 소 및 시 설 |
|---|---|
| 1 | 선교(Navigational bridge) |
| 2 | 중앙제어장소(Control stations and central control station) |
| 3 | 주요 기계설비Machinery space(main engine, generator, steering gear 등 ) |
| 4 | 물탱크, 펌프, manifold와 연결 장소 |
| 5 | 화물 펌프 실 |
| 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 Table 4와 같은 요건을 가진 선박보안경보시스템(ship Alert System)의 설치가 필요하다.

Table 4 Requirements for ship alert system

| 구분 | 요 건 |
|---|---|
| 1 | 주 관청이 지정한 책임당국에 보안경보를 송신 |
| 2 | 선상에 경보의 송신 무인지(무 알람) |
| 3 | 다른 선박에 경보신호 무 전송 |
| 4 | 임위적인 재설정 할 때까지 지속적인 보안경보신호 발생 |

(2) 선박의 식별 및 관리를 위하여 선박식별번호(Ship identification Number)를 영구적으로 표시되어야 한다.

(3) 보안정보를 국제적으로 통합 관리하여야 한다.

(4) 테러억지 지원세력(해군, 해경) 협력 체제를 구축해야 한다.

2.2.5 보안위험 기반으로 능동적 선박 운항 제어

(1) 선박자동식별시스템(Automatic Identification System: AIS 조기 도입을 통한 선박의 위치 추적을 해야 한다.

(2) 선박이력기록부(Continuous Synopsis Record: SCR) 도입하여 선박의 과거 행적 및 사건에 관한 정보를 기록 관리해야 한다.

(3) 회사보안검사관(CSO)이 전 자사 선박 보안관리를 일원화하고 그 에 관한 권한과 책임 부여해야한다.

2.3 선박보안위험 종류

선박의 잠재적인 보안위협 종류는 다음과 같다.

(1)테 러: 선박을 자체 무기로 이용하여 육상의 타 시설을 공격하거나 화학무기를 비롯한 대량테러 무기의 수송수단으로 이용이 가능하다. Fig. 1은 해양산업별 테러리스트에 의한 위협 가능성에 대한 조사 내용이다. Connecticut 해운회사조합(CMS)이 실시한 업계 관계자에 대한 설문조사에 따르면 container 화물이 수송량 증가와 더불어 검사의 어려움의 이유에서 테러위협에 가장 크게 노출되는 것으로 인식되고 있으며 항만에서의 선박 폭파 위협이 그 다음으로 나타나고 있다.

(2)무장해적: 여러 지역(항만, 협수로, 연안항해)에서 상선에 심각한 보안위협 되고 있다. Fig. 2 및 Fig. 3은 주요 해적발생 지역과 빈도를 나타낸다.

(3)마약유통: 마약의 생산지로부터 마약의 운반 및 판매에 관련된 행위로 중남미 해역, 동남아시아 해역에서 해양이 마약의 유통 경로로 이용되는 경우가 증가하고 있다.

(4)무기유통: 불법으로 총기류, 폭발물, 방사선 물질, 생화학무기를 비롯한 대량 살생무기의 운반 및 유통 행위로 갱단, 테러집단에 의한 해상유통위협이 증가하고 있다.

(5)밀항: 적합한 출입국 절차 없이 선박을 통하여 해외로 이동행위로 전통적인 해상보안위협으로 인식되고 있으며 선진국에 집중되는 현상을 보이고 있다.

(6)납치: 승무원의 안전 위협대가로 정치적, 금전적 대가 요구 행위이다.

(7)파괴행위(vandalism): 특정 목적 혹은 요구불만 등의 정신불안으로 선박의 파괴나 침몰시키는 행위이다.

(8)노동자의 단체 행동: 노동 종사자들의 집단적인 권리 주장 행위로 선박의 정상적인 운항에 지장을 초래한다.

(9)승무원의 폭력 및 폭동: 우발적인 감정의 대립으로 인한 개인적인 폭력행위 또는 요구불만에 대한 집단적인 폭력에 의한 집단행동이다.

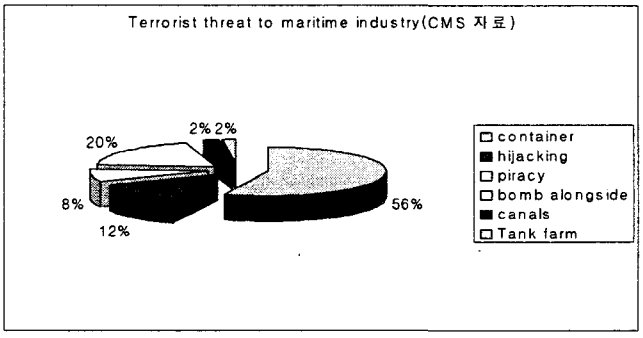


Fig. 1 Terrorist threats to maritime industry

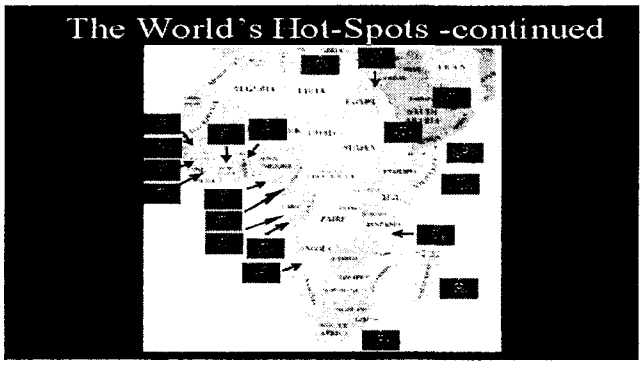


Fig. 2 Places and frequency of pirates(1)

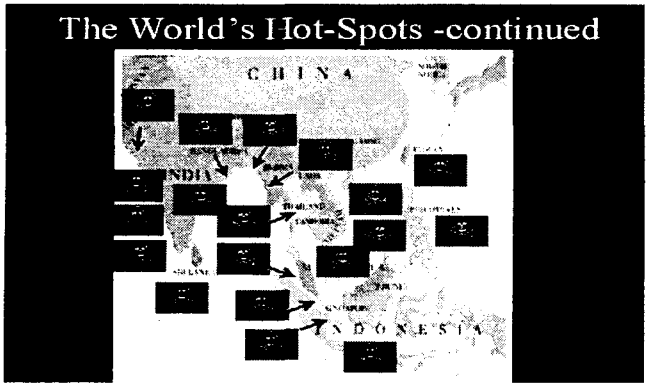


Fig. 3 Places and frequency of pirates(2)

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 보고 되고 있다. 밀항도 심각한 해상보안위험으로 등장하고 있는 실정이다.

## 3.선박보안위험관리 (SecurityRiskManagement)

### 3.1선박 보안위험 평가

선박보안 평가란 보안위험을 줄이기 위하여 보안위협에 대한 보안 위험을 평가하고 보안조치를 결정하는 과정이다. 일반적으로 선박보안위험(Security Risk: R)은 보안사고의 가능성(Frequency: F)과 사고에 의한 피해의 심각성(Consequence: C)의 두 변수로 다음 식과 같이 표현할 수 있다.

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

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

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

따라서, 선박보안 보안위험은 다음과 같이 표현된다.

$$R = T * C * V \quad (3)$$

### 3.2 Ship Security Risk Management

국내에서는 해상보안업무에 대한 책임은 보안공격에 대한 억지세력을 보유한 군대 혹은 경찰에 있는 것으로 인식되어 왔다. 그 결과 사고의 심각성에 비하여 다른 형태의 위험(Risk)과는 달리 최근까지 해상근로자에게 큰 관심의 대상이 되지 못하였다. 선박에 대한 테러와 같은 보안공격은 자연재해위험, 안전사고위험, 재정위험 등과는 다른 형태의 위험이지만 동일 기법으로 위험을 효과적으로 관리하기 위하여 Fig. 4와 같은 Ship Security Risk Management System를 도입할 수 있다.

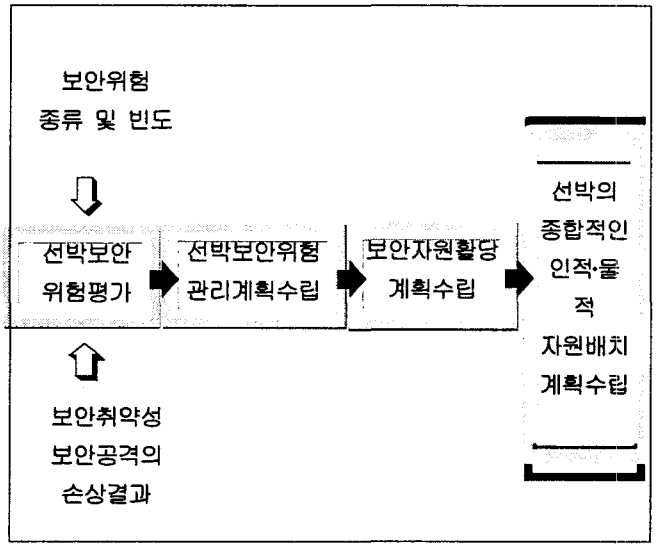


Fig. 4 Overview of ship security risk management system

### 3.3 위험 평가와 의사결정 시스템

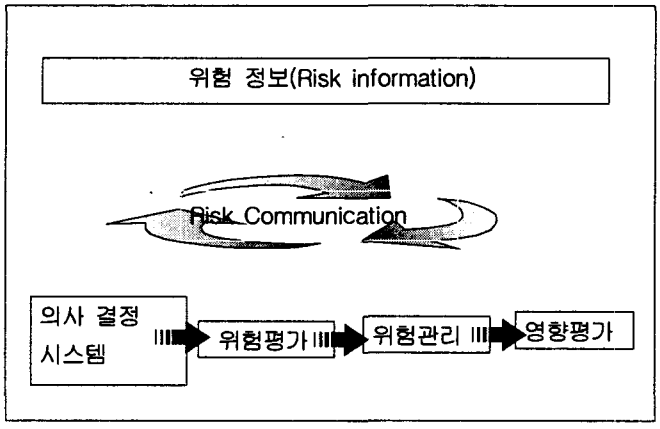


Fig. 5 Risk-based decision-making process

해상에서 선박이 직면할 선박 보안 사건에 대하여 올바른 보안위험 평가를 바탕으로 유효하고, 실현 가능한 효과적인 의사결정을 하기 위하여서는 적절한 정보수집방법과 구조화된 의사결정 시스템이 필요하다.

Fig. 5는 위험기반 의사결정과정과 시스템의 개념을 나타낸다. 위험기반의사 결정은 다음 순서로 이루어질 수 있다. 구조화된 의사결정 시스템을 바탕으로 첫째, 다양한 정보교환 인터페이스로 위험정보를 수집·가공하고 위험을 인지한다. 둘째, 컴퓨터를 활용하여 프로그램화된 위험 평가기법으로 선박보안 위험을 평가한다. 셋째, 위험회피, 위험제거, 위험분산 등으로 위험을 제어 관리한다. 넷째, 위험관리의 결과를 평가함으로써 각 단계별 개선방법을 강구해 나간다..

## 4.선박의보안모델

### 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 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. Table 5는 승무원의 보안업무의 분담의 예를 나타낸다. 보안위험을 사전에 인지하고 예방하기 위한 조치는 물론 보안공격 대비한 체계적인 대응조치와 사후 처리에 대하여도 합리적이고 실행가능한 조직의 구성과 업무 분담이 이루어져야 한다.

#### 4.1.2 Prevention Through Crew Program (PTC)

일반적으로 상선은 보안공격에 대해서 자기방어를 위한 무기체계를 가지고 있지 않다. 또한 항구 이외에서 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 해역에서 고립성을 가지고 운항되는 상선의 보안위험을 낮추기 위해서는 무엇보다도 승무원의 의한 테러예방 및 대응 프로그램 구축이 필요하다. Table 6은 승무원에 의한 테러예방 (PTC) 프로그램의 예시를 나타낸다.

Table 5 Ship security organization and duty

| 구분 | 직책 | 임무 | 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 | |

Table 6. Prevent Through Crew program

| 구분 | 목표 | 내 용 |
|---|---|---|
| 1 | Know More | 선박의 보안 위험의 종류, 취약성 |
| | | 테러대응기술, 보안위험관리법 등 |
| 2 | Train More | 테러대응훈련, 보안장비사용법, 보안점사법 |
| | | 위험물 취급 및 식별 법, 무기류 사용법 |
| 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

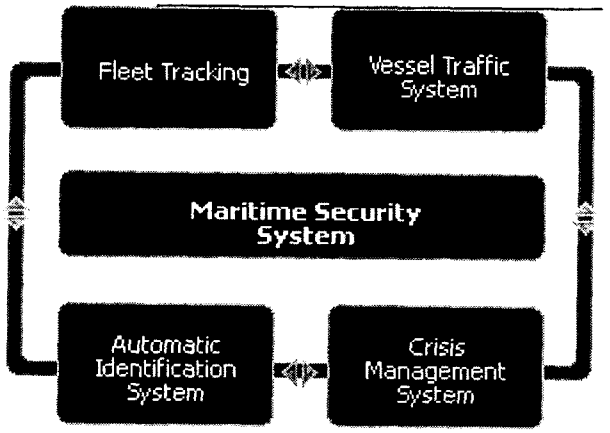


Fig. 6 Diagram of maritime security system

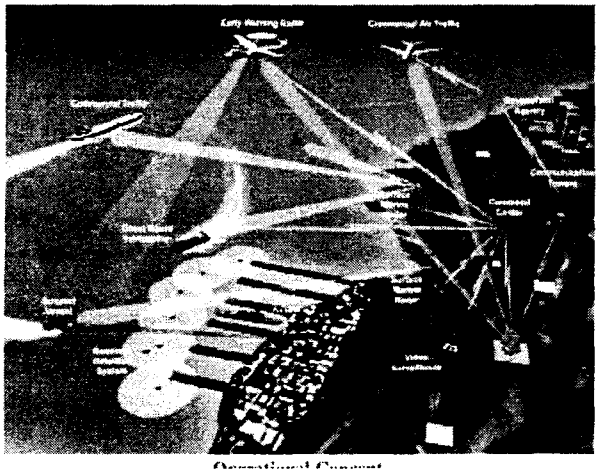

Fig. 7 Overview of maritime security system

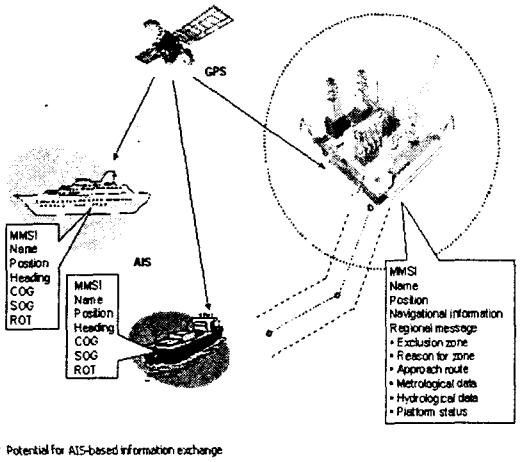


Fig. 8 Automatic Identification System

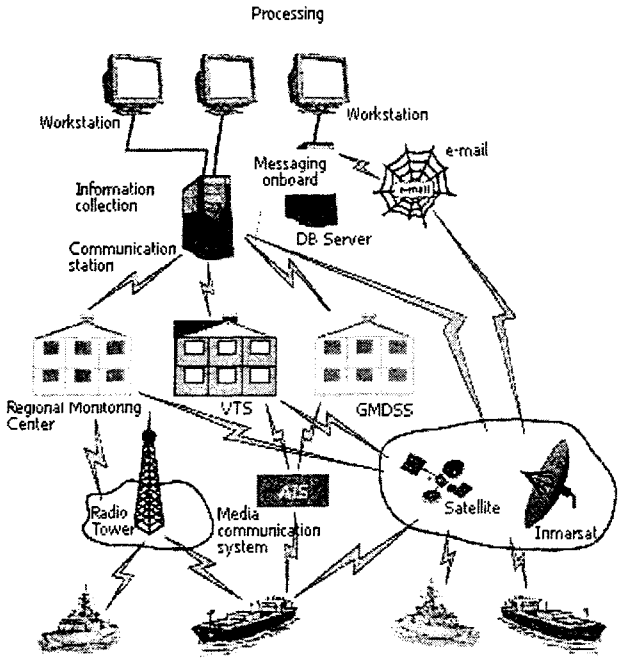


Fig. 9 Ship monitoring system

Fig. 6는 선박 모니터링, VTS, AIS로 구성된 해양보안 시스템의 개념도이며 Fig. 7은 Radar와 위성, AIS ,항공기, 통신망, 네트워크를 활용한 해양보안 시스템으로 현재 미국에서 운영하고 있다.[12][13][14][15]

Fig. 8은 2004년 7월 1일부터 SOLAS 협약에 의거 탑재가 강제되는 AIS (Automatic Identification System) 개념도이다. 선박이나 해양시설부터 실시간에 보안에 필요한 정적, 동적 정보를 수집할 수 있다. Fig. 9는 AIS, 통신위성, VTS, 통신 시스템을 이용한 선박 모니터링 시스템을 나타낸다.

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. Fig. 10은 선박보안 시스템 구성도 이다. 선박의 보안 시스템은 출입자의 출입을 통제하는 출입보안 시스템, 선박주위 및 주요 시설물의 감시를 위한 감시 시스템, 보안공격에 의한 피해를 최소화하기 위한 대응 시스템, 외부 지원 세력의 지원과 공동 대응을 위한 외부 지원 시스템으로 구성될 수 있다. 세부 구성 구성요소들은 다음과 같다.

(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, 비상통신망, 외부지원세력 등.

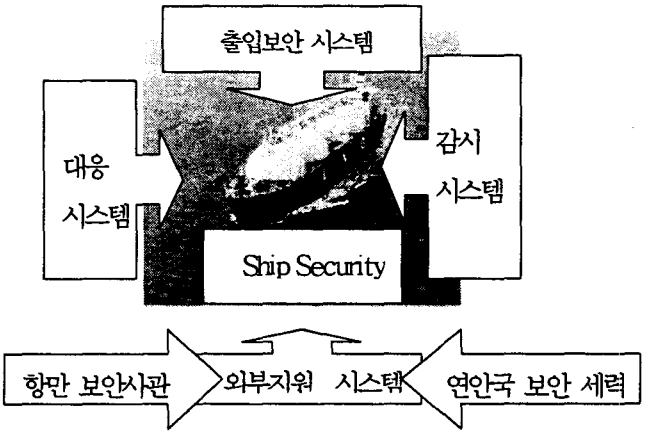


Fig. 10 Ship security system

## 5.결 론

미국의 테러사건 이후 해양산업과 상선에 대한 테러 경각심이 높아지고 있다. 자체의 방어 무기체제 없이 광활한 해상을 활동 무대로 하는 상선은 인명, 선박과 화물의 재산, 환경 및 경제에 미치는 직·간접 영향의 광대성 때문에 테러의 목표물

이나 수단으로 사용될 개연성이 높다.

본 논문에서는 상선에서 보안 사고를 예방하고 보안위협에 대하 효과적으로 대응하기 위하여 해양보안위협과 선박의 보안관리 특성을 분석하고 선박보안관리 원칙을 도출하였다. 또한 해양보안시스템과 보안모델을 고찰하고 위험관리 기법을 도입하여 선박보안위험의 체계적인 관리방안을 제시하였다. 그리고 발효가 예정된 ISPS 규정에 입각하여 선내의 보안조직과 보안업무를 설정하고 승무원의 보안문화 정착을 위한 PTC 프로그램을과 선박의 보안 시스템을 구성하였다.

앞으로는 해양에서 보안취약성을 보완하고 보안위험을 낮추기 위해 선박의 특성을 고려한 보안 시스템 및 보안장비의 개발에 관한 연구를 계속적으로 수행할 예정이다. 항만, 연안, 영해에서 선박의 보안수준을 높이고 체계적인 대응을 위하여 보안 지원세력의 일원화와 체계적인 해안 보안 시스템의 구축에 국가적인 노력이 요망된다.

원고접수일 : 2003년 4월 15일
원고채택일 : 2003년 6월 18일

## 참고문헌

[1] 해양경찰청, "중장기 해상종합치안 수요전망과 대책방안 용역보고서", 2002.7.

[2] IMO, "International Ship and Port facility Security Code (ISPS)", 2003 Edition, 2003.

[3] 신의기, "해상테러억제를 위한 로마협약에 관한 고찰, , 형사정책연구", 제9권 제1호(통권 제33호1998 봄호).

[4] 해양경찰청, "해양경찰기능 및 조직체계 개선방안 연구 용역보고서", 2001. 12.

[5] Bruce B. Stubbs, "The Coast Guard and Maritime security", JFQ, 2000.8.

[6] United States Coast Guard, "Navigation and vessel inspection circular No.1002" , 2002.

[7] Connecticut Maritime Association, "Maritime Security Survey Result", 2002.

[8] ICC, " Piracy report", 2002.

[9] Vernon H. Guthrie, David A. Walker, "Modeling Security Risk", ABS Consulting, 2002.

[10] USCG, "Advancing the principle of the prevention through people program" , 1997.

[11] USCG, "Prevention Through People (QAT report), 1995.

[12] Navi-Guard security System, http://www.transas.com/products/navi_guard

[14] Maritime Security System, http://www.lockheedmartin,com

[15] 해양수산부, "선박자동식별장치)AIS) 도입 위한 기초연구평가용역 보고서", 2001.

[16] Transa company homepage, http://www.trasas.com