# 선박사이버보안 계획서 및 대응체계 비교에 대한 연구

안영중* · 김보라** · † 박성호

*,† 한국해양대학교 항해융합학부 교수, **한국해양대학교 대학원

**요 약** : IMO는 해상사이버보안 관리기준을 제정하여 2021년부터 ISM code에 따른 선박안전관리 지침 상 사이버보안 관리방안의 반영을 권고하였다. 이에 따라 선박에 대한 사이버보안 관리지침 또는 계획서 등이 선박회사별로 개발되어 적용되어 오고 있으나 명확한 법적 근거 및 표준이 부재하여 선박회사별 차이가 발생하고 있다. 본 연구는 국내 선사들의 사이버보안 계획서를 BIMCO, NIST 등의 Guideline과 Framework 기반으로 비교하여 선사별 사이버보안 대응을 위한 선내조직 및 역할과 책임, 비상 시 대응방안을 비교하였다. 비교 결과를 기반으로 차이점과 개선점 식별을 통해 실효성 있는 사이버보안계획서 수립 및 대응조직 구성 방안제시를 연구목적으로 설정하여 수행하였다.

**핵심용어** : 사이버보안, 사이버보안 계획서, 대응조직, 비상대응

## 1. 연구개요

### 1.1 연구배경

- IMO는 해상사이버보안 관리기준을 제정, ISM code에 따른 선박안전관리 지침 상 사이버보안관리방안의 반영 권고(관리 필요성), 이에 따라 선박에 대한 사이버보안관리지침 또는 계획서 등이 선박회사별로 개발되어 적용
- 물리적 선박보안관리의 경우 보안계획서의 내용과 대응체계에 대한 근거가 국제협약(SOLAS 11-2, ISPS Code)으로 명확함에 비해 사이버보안관리 계획과 대응체계에 대한 근거 미비로 선사별 개발된 내용과 수준이 상이함




## 2. 선박사이버보안 계획서 비교

### 2.1 사이버보안관리의 적용 비교 (1)

- 국내 8개 선박회사 대상의 사이버보안관리 현황 조사 수행
  → Cyber Security Instruction / Guidance / Procedure / Plan 등 다양한 명칭으로 사이버보안관리 방안을 선박에 제공

| | 명칭 | 비고 |
|---|---|---|
| A 사 | Cyber Security Instruction | 컨테이너선사 |
| B 사 | Cyber Security Operation Guidance | 컨테이너선사 |
| C 사 | Cyber Security Procedure | 벌크선사 |
| D 사 | Cyber Security Response Plan | 탱커선사 |
| E 사 | Cyber Security Procedure | 탱커선사 |
| F 사 | Cyber Security Response Plan | 탱커선사 |
| G 사 | Cyber Security Procedure | 벌크선사 |
| H 사 | Cyber Security Operation Guidance | PCC선사 |



## 1. 연구개요

### 1.2 연구목적

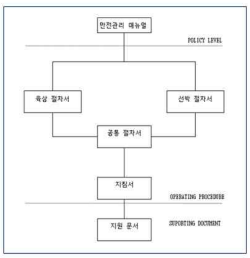
- BIMCO, NIST 등의 Guideline과 Framework 기반으로 선박회사별로 개발된 사이버보안계획서 또는 선사 절차서 등을 비교하고,
- 선사별 사이버보안 대응을 위한 선내조직 및 역할과 책임, 비상 시 대응방안 비교하여 차이점과 개선점 식별을 통해
  → 실효성 있는 사이버보안계획서 수립 및 대응조직 구성 방안제시




## 2. 선박사이버보안 계획서 비교

### 2.1 사이버보안관리의 적용 비교 (2)

- ISM code에 따른 선박안전관리 지침 상 사이버 보안관리의 반영 여부 검토
  → 절차서 또는 지침서 수준에서 Cyber Security 관리방안 반영 중




IMO 권고에 따라 안전관리 매뉴얼 하위의 절차서 또는 지침 형태로 사이버 보안을 적용하고 있는 부분은 공통적이며, ISPS Code에 근거한 일반 보안관리와는 다르게 선박안전관리의 일환으로 적용

Guidance와 같이 지원문서의 성격으로 적용하고 있는 선사(B사, H사)가 일부 있었으며, 구체적 내용 및 분량에 있어서 8개 선사 모두 차이를 보였음, 적용 시기는 탱커선사들이 18/19년으로 앞서 적용



† 교신저자 : 정회원, shpark@kmou.ac.kr, 051)410-4232
* 종신회원, yjahn0726@kmou.ac.kr, 051)410-4235

## 2. 선박사이버보안 계획서 비교

### 2.2 구성 비교

◆ BIMCO의 가이드 라인 CRMA(Cyber Risk Management Approach) 요소에 대한 비교 검토 → 관련 항목별 적용 사항은 선사마다 차이가 있음

| | Contents | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|---|
| CRMA-01 | 위험의 식별 | X | O | O | O | O | O | O | O |
| CRMA-02 | 취약성의 식별 | O | O | X | O | O | O | O | X |
| CRMA-03 | 리스크 평가 | O | O | O | O | O | O | O | △ |
| CRMA-04 | 보호 및 탐지 방법 개발 | △ | △ | O | O | △ | O | △ | △ |
| CRMA-05 | 비상계획의 수립 | O | △ | △ | O | O | △ | O | O |
| CRMA-06 | 보안사고 대응 및 복구 | O | △ | X | △ | O | △ | O | O |

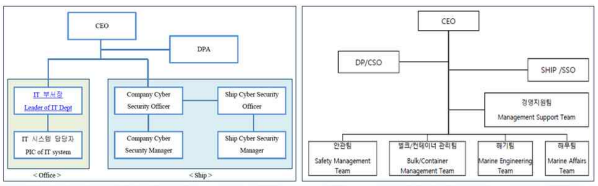
O : 가이드 라인의 내용을 인용하고, 해당 선종의 특성을 고려하여 작성
△ : 가이드라인의 내용을 인용하였으나, 해당 선종의 특성 미반영 또는 제시안 없음
X : 가이드라인 내용의 인용도 없고, 해당 선종의 반영 및 제시안 없음



## 3. 사이버보안 사고 대응체계 비교

### 3.1 사이버보안 사고 대응조직

◆ 사이버보안 사고 발생 및 관리를 위한 역할 및 책임 지정 검토
→ 8개 선사 모두 명시, 선박대응책임자 및 회사 대응책임자도 지정되어 있음
→ SSO로 지정된 경우와 CySO 명칭 사용이 혼재, 주로 선장 지정
◆ 사이버보안 대응을 위한 육상 전문인력 또는 조직 지정 여부 검토
→ 1개 선사만이 별도의 IT 담당 육상부서 지정



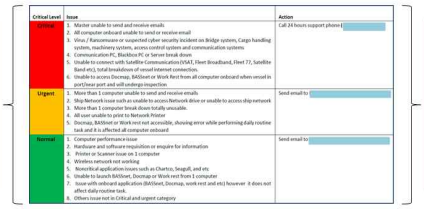



## 3. 사이버보안 사고 대응체계 비교

### 3.2 사이버보안 연락망 구성

◆ 사이버보안 관리 및 대응을 위한 육해상 간 연락망 구성 여부
→ 5개 선사 연락망 구성, 3개 선사는 연락망 부재함
→ 선박과 육상 간 연락 절차와 대상 및 시기를 제시한 회사는 1개 선사 유일

Critical 수준 결정 (이슈 제시 연락 필요 상황을 명시)




Critical 수준별 연락방법과 대상 제시



## 4. 연구결과

### 4.1 연구사항 요약

◆ 사이버보안 관리현황에 대해 가이드라인 적용, 비상 대응조직 구성과 역할 임무지정 및 비상대응계획의 실효성과 구체성에 대한 비교 수행
→ 비상대응 실효성과 구체성에 대한 연구진의 정성적 평가가 반영되었으나, 여러 선사들의 사이버보안관리의 차이 비교 목적

| Contents | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 가이드라인 적용 (6개 항목) | 4.5 | 4.5 | 3.2 | 5.5 | 5.5 | 5.0 | 5.5 | 4.0 |
| 대응조직 구성 및 역할 지정 (4개 항목) | 4.0 | 3.0 | 3.0 | 4.0 | 4.0 | 4.0 | 4.0 | 3.0 |
| 비상대응 연락망 실효성 (5점 척도 비교) | 3.5 | 4.0 | 4.0 | 4.5 | 4.5 | 5.0 | 4.0 | 4.5 |
| 비상대응계획의 구체성 (5점 척도 비교) | 3.5 | 3.0 | 3.0 | 4.0 | 4.5 | 4.5 | 4.0 | 4.0 |



## 4. 연구결과

### 4.2 사이버보안계획서 실효성 향상 방안 (1)

◆ 선사별 사이버보안계획서 검토를 위한 Cross reference table 제시
→ 사이버보안관리 방안에 반영되어야 하는 IMO 문서 및 국제가이드라인, 주요 선급 지침사항 반영을 점검 가능한 Table 구성 제공 필요
→ 선사별 사이버보안관리 수준 차를 줄이고, 필수적 사항 누락 방지
◆ 선박별 자산 평가 기반의 취약성 검토 및 리스크 관리
→ 각 선박별 자산(Asset) 평가 없이 공통적 IT/OT 기기에 대한 리스크 평가로 인해 대응조치의 구체성/실효성에 대한 문제점 식별
→ On-Scene Survey 및 전문적 평가 가능 조직에 위임, 자산 목록화 방안
◆ 사이버 대응조직 구성에 해당분야 전문성 확보 고려
→ 사내 IT 담당 팀 또는 전문적 외부 자문이 가능하도록 조직도 구성 필요
→ 사이버보안 사고들은 피해 저감을 위해 전문적 대응을 필요로 함



## 4. 연구결과

### 4.2 사이버보안계획서 실효성 향상 방안 (2)

◆ Contingency plan의 Flow chart와 절차의 유형별 대응계획 제시
→ 사이버보안 사고 발생 시 관련 전문성이 부족한 선원들의 효과적 대응을 위한 위협이나 공격 상황별 대응 절차와 순서도 제시 필요
◆ 선박보안 대응담당자 대상의 사이버보안 교육훈련의 전문성 필요
→ 탱커선사들의 사이버보안관리사항에만 선박 근무자들의 교육 훈련 근거와 교육 시기 및 대상, 교육 내용들이 제시되어 있음
◆ 사이버 보안위협의 단계적 상황별 연락망 구성
→ Critical 수준별 연락 방법과 대상 제시 사례, 사이버 보안위협 수준을 세부적으로 구분하고 각 수준에 적합한 연락대상과 보고방법을 제시하여 대응 효율성 향상