

Vol. **71**

2022년 10월  
**해사안전**

# IMO 국제해사 정책동향

IMO 국제해사 정책동향은 해양환경, 해사법률, 해사정책, 해사안전, 전략계획 등의 콘텐츠를 기반으로 최신 동향을 소개하는 발간물로, 한국해양수산개발원 홈페이지([www.kmi.re.kr](http://www.kmi.re.kr))에서도 확인하실 수 있습니다.

- 총 괄 박한선 실장
- 감 수 이연경 연구위원
- 발행인 김종덕 원장
- 발행처 물류·해사산업연구본부  
해사산업연구실
- 주 소 49111 부산광역시 영도구 해양로  
301번길 26(동삼동)
- T E L . 051-797-4800
- F A X . 051-797-4810



**한국해양수산개발원**  
KOREA MARITIME INSTITUTE

## 해사산업 분야의 디지털 기술 개발, 사이버보안과 함께 가야

### IMO, 선박 디지털화에 따라 사이버 공격 대응 마련을 위한 노력 가속화

#### ▶ IMO는 법적 프레임워크를 마련하기 위한 워크숍 개최<sup>1)</sup>

- IMO는 에티오피아에서 10월 10일-14일, 5일 동안 해사 보안을 위한 워크숍을 개최함
- 워크숍은 EU가 지원하는 지역프로그램 'Red Sea Project(The Regional Programme for Maritime Security in the Red Sea Area)<sup>1)</sup>'의 일환으로 진행됨
- 워크숍은 MSC.1/Circ.1525<sup>2)</sup>, SOLAS Chapter XI-2 및 ISPS Code에 대한 이해와 적용 방안 위주로 진행됨
- 주최는 에티오피아 해양청(EMAA: Ethiopian Maritime Affairs Authority)이며, IMO의 적극적인 지원을 통해 워크숍이 개최된 만큼 IMO의 해사 안전과 보안을 위한 노력이 엿보임

〈그림1〉 Boosting maritime security in Ethiopia



자료 : IMO

1) Red Sea Project는 홍해와 접촉된 나라(수단, 예멘, 에티오피아, 소말리아, 지부티 등)의 해사 보안에 관련한 국제해사법, 항만보안 관리시스템, 항만국 통제, 해사 보안 조치의 영역에서 지원함  
2) 국가 해양보안법 개발을 위한 지침

### ▶ IMO와 IACS(국제선급협회)<sup>3)</sup>의 사이버보안 조치

- IMO는 2022년 6월, MSC-FAL.1/Circ.3/Rev.2을 통해 새로운 형태의 해사 사이버 위협 대응에 대한 가이드라인을 제시함
- 해당 가이드라인은 해사산업의 정보통신, 데이터 교환 및 해양 디지털기술의 고도화는 효율 향상 측면에서는 효과가 상당하지만, 악의적인 사이버 위협에 더 쉽게 노출되는 단점이 있음을 강조함
- IACS는 해양 사이버 보안에 대한 새로운 UR(Unified Requirements)인 E26 및 E27<sup>b)</sup>을 발표했음
- E26의 경우 선박의 사이버 복원력(Cyber Resilience)을 위한 식별, 보호, 탐지, 대응, 복구 측면의 공통 규칙이고, E27의 경우, 선박의 온보드시스템과 장비의 사이버 복원력에 관한 내용을 담고 있음
- IACS는 2024년 1월 1일 이후에 건조계약을 맺은 선급 선박 및 해양 설비에 대해 사이버 위협 대응은 의무사항임을 발표함<sup>c)</sup>
- IACS UR E26 및 E27의 기술적 충족요건은 DNV<sup>4)</sup>의 사이버보안 등급인 Cyber Secure(Essential)과 동일하며, 결과적으로 Cyber Secure(Essential)이 의무화된다고 볼 수 있음
- Cyber Secure는 필수적인 보안인 Entry를 기본으로 Essential, Advanced, (+)로 구분되어 있고, 선박의 추진, 조향, 발전, 항법 등을 포함한 10가지 선박 필수 기능을 취급함

## ■ 해사산업, 사이버위협은 또 다른 재해

### ▶ 해사산업의 사이버 보안관련 피해 사례 증가 중

- 자율운항선박 및 스마트 항만 개발에 따른 해사산업의 디지털화로 인하여 사이버 보안관련 위협과 테러의 우려가 가중됨
- 세계에서 가장 분주한 항만 중 하나인 미국 LA항은 Covid-19 펜데믹 이후로 월간 사이버 공격이 약 4천 건 이상으로 2배 이상 증가함<sup>d)</sup>
- 대표적으로, 2017년 머스크사의 터미널 IT 시스템이 랜섬웨어 공격으로 인하여 3주간 시스템 마비, 약 3천억 원의 피해를 입은 사례가 있음
- 그 이후로도 바르셀로나항, 샌디에고항 등과 같은 항만의 피해 사례 뿐만아니라, 선박의 항해 시스템, IT 시스템 해킹으로 인한 통제권 상실, 시스템 포맷과 같은 피해도 발생함
- Sembcorp Marine社は 승인되지 않은 소프트웨어를 통해 네트워크에 접근하는 사이버 공격을 발견하여 초기에 즉각적인 대응으로 인하여 큰 피해를 입지 않았음<sup>e)</sup>
- 해사산업 분야에서의 사이버 보안관련 사고는 금전적 피해뿐만 아니라, 선박의 통제권 상실로 인한 인명

3) International Association of Classification Societies (국제선급협회)

4) Det Norske Veritas (노르웨이 선급)

피해까지도 일으킬 수 있기 때문에 사전 대응이 중요함

## ■ 해사산업의 사이버보안 기술과 시스템 강화를 위한 노력 촉구

### ▶ 해사산업 분야의 디지털전환 속도에 맞추어 사이버보안에 관한 전략 마련 필요

- IMO MASS(Maritime Autonomous Surface Ship) Code 개발의 노력이 활발하게 진행되는 시점에서 사이버보안의 중요도가 더 커짐
- 현재까지의 해사산업 분야의 사이버 위협은 주로 항만 시스템을 대상으로 진행되었지만, 자율운항선박 및 무인화선박의 상용화가 가까워질수록 선박 탈취, 고의적 선박 충돌 유발 등의 우려가 커지고 특히, 승객이 승선한 여객선의 경우에서의 사이버위협은 그 피해가 가늠이 안 되는 수준임
- 사이버보안 체계를 완벽히 구축해도 계속해서 진화하는 사이버 위협, 시스템 해킹, 사이버 테러의 특성상 지속적인 보안 시스템의 개발과 발전이 중요하다고 판단됨
- 현재 해사분야 사이버보안 전문가가 부족하기 때문에 해당 전문가를 양성하고 인증하기 위한 교육훈련 및 인증제도를 개발하여 해사산업 사이버보안 시스템의 지속적인 개발과 발전을 가능케 해야함
- 또한 자율운항선박 개발에 따라 원격제어자 및 해상교통관제 관계자들을 위한 해사 사이버 보안 교육훈련을 실시하는 것도 대응 방법이 될 수 있다고 생각됨

김지호 연구원

물류·해사산업연구본부 해사산업연구실  
(jiho@kmi.re.kr / 051-797-4662)

### 참고 자료

- <https://www.imo.org/en/MediaCentre/Pages/WhatsNew-1766.aspx> (검색일 : 2022.10.18.)
- <https://iacs.org.uk/publications/unified-requirements/ur-e/?page=2> (검색일 : 2022.10.18.)
- [https://www.dnv.com/news/iacs-unified-requirements-for-cyber-security-mandatory-from-1-january-2024-227429?utm\\_campaign=MA\\_22Q2\\_TRN\\_No\\_17\\_EXT\\_IACS%20Unified%20Requirement%20for%20cyber%20security&utm\\_medium=email&utm\\_source=Eloqua](https://www.dnv.com/news/iacs-unified-requirements-for-cyber-security-mandatory-from-1-january-2024-227429?utm_campaign=MA_22Q2_TRN_No_17_EXT_IACS%20Unified%20Requirement%20for%20cyber%20security&utm_medium=email&utm_source=Eloqua) (검색일 : 2022.10.19.)
- <https://safety4sea.com/port-of-la-cyber-attacks-have-doubled-since-pandemic/> (검색일 : 2022.10.19.)
- <https://safety4sea.com/sembcorp-marine-hit-by-cyber-security-incident/> (검색일 : 2022.10.19.)