Vol.126 2023년 11월
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)에서도 확인하실 수 있습니다.

총 괄 박한선 실장
감 수 이언경 연구위원
발행인 김종덕 원장
발행처 물류·해사산업연구본부 해사산업연구실
주 소 49111 부산광역시 영도구 해양로 301번길 26(동삼동)
TEL. 051-797-4800
FAX. 051-797-4810

KMI 한국해양수산개발원
KOREA MARITIME INSTITUTE

해사 사이버 위험에 대처하기 위한 역량 강화 필요

IMO, 사이버보안에 대한 관심을 촉구하고 사이버 위험관리를 위한 노력 지속

- IMO와 플리머스(Plymouth) 대학 Cyber-SHIP Lab은 공동으로 '해사 사이버보안과 복원력(resilience)'에 관한 공동 심포지엄을 개최 [a),b)]

- 2023년 11월 1~2일 런던 IMO 본부에서 개최된 공동 심포지엄에서 최신 국제 해사 사이버위험 평가와 위험 완화 연구를 공유하고 정부, 산업계, 연구자와 NGO가 국제 해사 공급망 사이버 복원력을 형성하기 위한 협력 방안 논의

* 복원력(resilience)은 사이버 공격과 같은 이벤트 등에도 불구하고 의도한 결과를 지속적으로 제공할 수 있는 능력을 의미

- 산업계·학계 전문가들은 자산과 사람의 안전, 신기술, 정책개발과 선원훈련을 포함하여 선박, 항만, 해사 공급망 전반에 걸쳐서 사이버보안을 다룸

- Cyber-SHIP 연구실은 플리머스 대학 사이버위협연구그룹(Cyber Threats Research Group)의 유일한 하드웨어 기반의 해사 사이버-물리 테스트베드(cyber-physical testbed) 시설임

〈그림 1〉 해사 사이버 보안과 복원력에 관한 심포지엄

자료 : IMO

- 심포지엄에서는 사고 보고체계, 사이버 보안 로드맵, 사이버-물리공간 연구 플랫폼, 사이버 복원력, 거버넌스와 규제 등에 대해서 논의

IMO는 해사 사이버위험에 대응하기 위하여 가이드라인을 제시 [c),d)]

- 해사 사이버위험(cyber risk)은 잠재적 상황이나 사건으로 인해 기술 자산이 위협받을 수 있는 정도를 의미하며 정보나 시스템의 손상, 손실로 인하여 운송과 관련된 운영, 안전 또는 보안 장애를 초래할 수 있음
- 사이버 위험관리(cyber risk management)는 사이버 관련 위험을 식별, 분석, 평가, 소통하고 이해관계자에게 미칠 비용과 편익을 고려하여 용인가능한 수준으로 수용, 회피, 이전 또는 완화하는 과정을 의미
- 사이버 위험관리의 전반적인 목표는 위험 없는 안전한 운항을 지원하며, 사이버 위험에 탄력적으로 대응하는 것이며 IMO에서는 이와 관련하여 MSC-FAL.1-Circ.3-Rev.2 가이드라인을 발행함
- 가이드라인은 현재 존재하거나 향후 발생할 사이버 위협과 취약점으로부터 선박을 보호하고 효과적인 사이버 위험관리를 지원하는 기능적 요소를 포함하여 해사 사이버 위험관리에 대한 높은 수준의 권고사항을 제공
- 해사안전위원회(MSC: Maritime Safety Committee)는 2017년 6월 98회 세션에서 안전관리시스템(Safety Management Systems)의 해사 사이버 위험관리 결의안 MSC.428(98)을 채택함
- 결의안 MSC.428(98)에 따라서 2021년 1월 1일 이후에 시행되는 선사의 안전관리적합증서(Document of Compliance) 인증 이전에 사이버위험이 안전관리시스템에서 적절히 관리되도록 각국 정부에 권고

증가하는 사이버 위험에 대비하여 선박의 사이버 복원력 확보 필요

사이버 보안은 디지털 전환의 가속화로 해사 산업에서 더욱 중요해지고 있으며 새로운 위협과 그에 대응한 규제 요구 사항 발생 [e),f),g),h)]

- 선박의 사이버 시스템은 IT(Information Technology)와 OT(Operation Technology)로 크게 구분되며, IT 부문은 대체로 사이버 보안에 대해 성숙한 편이며, 정보보안관리시스템(ISMS: Information Security Management System)을 사용하여 확립된 절차, 기술 및 교육을 적용하고 있음
- 반면에 OT는 사이버 보안에 관한 성숙도가 떨어지는 편이며, 선내 OT 시스템에 대한 공격은 선박의 안전과 선원의 생명을 위협할 수 있기 때문에 이에 대한 철저한 준비가 필요
- 사이버 공격은 맬웨어(Malware: 악성 소프트웨어)를 이용한 데이터 수집, 온라인 시스템의 전부나 일부를 다운시킨 후 금전 요구, 대가를 요구하지 않는 파괴적인 공격 등 다양한 형태가 존재하며, 회사에 보내는 공급자의 송장 이메일을 가로채어 다른 은행 계좌를 보내는 유형도 있음
- 해사 사이버공격 중 잘 알려진 사례는 2017년 NotPetya라는 맬웨어로 인해서 머스크(Maersk) 라인이 입은 피해로서 네트워크를 복구하는데 며칠이 걸렸으며, 약 2~3억 달러의 손실을 입은 것으로 추정됨
- 2021년 3월 일본에 본사를 둔 K Line은 맬웨어 공격을 받아서 기업의 엔터프라이즈 시스템이 일시적으로 중단되어 4월 중순에야 복구를 완료함
- 2021년 6월에는 우리나라의 대우조선해양 내부망에 대한 해킹 시도가 있었던 것으로 언론을 통해 알려짐

국제선급협회는 사이버 복원력에 관한 규정을 제정하여 사이버 위험을 관리하기 위해 노력 [i),j),k)]

- 사이버 복원력(cyber resilience)은 선박의 안전한 운항을 위해 사용되는 운영기술(OT: Operational Technology)의 중단·손상으로 야기되는 사이버 사고의 발생을 줄이고 그로 인한 영향을 완화하는 능력
- 국제선급협회(IACS: International Association of Classification Societies)는 2022년 공통요구사항(UR: Unified Requirements) E26 '선박과 사이버 복원력'과 UR E27 '선내 시스템과 설비의 사이버 복원력'을 발간

* UR E26, UR E27은 2024년 1월 1일 이후 신선부터 적용할 예정이었으나, IACS는 보도자료를 통해 2024년 7월 1일 이후 건조계약이 이루어지는 신선에 대해 적용하기로 변경

- IACS는 최소한의 기능과 성능 기준으로서 UR E26과 UR E27을 제시하였으며 선내의 OT 시스템, 즉 물리적 프로세스를 통제하고 모니터링하기 위해 데이터를 사용하는 컴퓨터기반시스템(CBS: computer-based systems)에 적용
- 사이버 사고에 취약할 수 있는 시스템에 적용하여 인명과 선박의 안전, 환경에 대한 위협으로부터 보호 목적
- 사이버 리스크에 대해 회복력이 있는 안전한 운항지원이라는 주요 목표를 달성하기 위해 5개의 기능에 따른 하부 목표를 설정
  - ① 식별(Identify): 선내 시스템, 인력, 자산, 데이터 및 기능에 대한 사이버 보안 위험을 관리하기 위한 조직적 이해 증진
  - ② 보호(Protect): 사이버 사고로부터 선박 보호와 운항 연속성의 최대화를 위한 적절한 보호장치 개발 및 실행
  - ③ 탐지(Detect): 선내 사이버 사고의 발생을 탐지하고 식별할 수 있는 적절한 조치 개발 및 실행
  - ④ 대응(Respond): 선내에서 탐지된 사이버 사고에 대해 조치를 취할 수 있는 적절한 수단과 활동 개발 및 실행
  - ⑤ 복구(Recover): 사이버 사고로 인해 손상된 선박 운항에 필요한 기능이나 서비스를 복구하기 위한 적절한 수단과 활동 개발 및 실행
- 이러한 하부 목표와 관련 기능 요소는 하나의 포괄적인 위험관리 프레임워크의 일부로 고려되어야 함

해사 사이버 위험에 대처하기 위한 다양한 이해관계자들의 대응 노력 필요

사이버 위험에 대처하기 위해 공공과 민간의 협력적 노력이 필요

- 정부는 IMO, IACS 등의 규제가 국내 선박의 건조, 운항 과정에 반영될 수 있도록 제도와 지침을 마련하는 것이 요구되며, 선사는 해사 사이버 위험관리 주요 지침 준수를 위한 인력 배치 및 구성원들에 대한 교육 강화 필요
- 선박의 IT와 OT 네트워크를 분리하여 위험 노출을 줄이고, 인증되지 않은 접근을 막기 위해 방화벽을 설치하고, 적절한 트래픽만이 네트워크에 허용될 수 있도록 제한된 접근만을 허용해야 함
- 선원들이 인터넷, 이메일, USB 등을 사용할 때 민감한 정보가 외부에 노출되지 않도록 보안수칙 교육을 강화하고, 네트워크를 사용할 때 암호화 등을 사용하여 보안을 강화해야 함

정재호 전문연구원
물류·해사산업연구본부 해사산업연구실
(chungjh@kmi.re.kr / 051-797-4391)

참고 자료

a) https://www.imo.org/en/About/Events/Pages/Symposium-Maritime-cyber-security-and-resilience.aspx (검색일 : 2023.11.07.)
b) https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (검색일 : 2023.11.07.)
c) IMO, MSC-FAL.1-Circ.3-Rev.2
d) IMO, MSC.428(98)
e) https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html (검색일 : 2023.11.07.)
f) KVH, 「Critical Considerations to Mitigate Cyber Risks at Sea」, 2023.
g) https://thetius.com/cyber-attacks-who-targets-the-maritime-industry-and-why/ (검색일 : 2023.11.07.)
h) https://www.nhlstenden.com/en/maritime-cyber-attack-database (검색일 : 2023.11.07.)
i) IACS UR E26
j) IACS UR E27
k) https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release (검색일 : 2023.11.07.)