



IMO 국제해사 정책동향



한국해양수산개발원
KOREA MARITIME INSTITUTE

Aug. 2018 발간년월 2018년 08월(통권 제8호) 주소 49111 부산광역시 영도구 해양로 301번길 26(동삼동) 발행인 양창호 원장
Vol. 7 감리 황진희 본부장 자료문의 한국해양수산개발원 해사안전연구실 홈페이지 www.kmi.re.kr

금주 Contents - 해사정책 이슈

해상 사이버 위험관리, 디지털 해사산업의 핵심 역량

2021년까지 ISM¹⁾ 코드에 사이버 위험관리를 반영하지 않은 선박은 억류조치

■ IMO 제98차 해사안전위원회('17.6.7~16)는 사이버 보안상의 위협과 취약성을 인식하여 해상 사이버 위험관리 지침(MSC-FAL.1/Circ.3)을 승인함

- 해상 사이버 위험관리는 디지털화, ICT 융합, 자동화 및 네트워크 기반시스템 의존도의 증가에 따라 해사산업(해운업, 항만업, 물류업 등)의 주요한 관리 항목임
- 사이버보안(Cyber Security) 기술은 선박안전과 해양환경 보호를 도모하기 위한 중요한 요소로 시스템의 접속, 상호연결 또는 네트워킹의 취약점 해결시스템을 포함하여야 함
- 또한, 해상 정보기술시스템은 선교시스템, 화물처리 및 승객서비스 관리시스템, 기계관리 및 전력제어 시스템, 접근제어시스템, 공공 네트워크를 사용하는 승객 관리, 행정 및 승무원 복지시스템, 통신시스템에 대해 악의적 영향(해킹이나 악성 소프트웨어의 전파)이 미칠 경우를 대비한 효과적인 사이버 위험관리를 포함하고 있어야 함

■ IMO는 선주와 선박관리회사에 사이버보안 및 위험관리에 관한 사항을 ISM Code에 반영하여 관리 및 운영하도록 강제적으로 시행하고 있음

- 사이버 위험관리를 위한 매뉴얼²⁾ 은 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)의 원칙에 입각하여 작성되어야 함

1) ISM(International Safety Management) 코드: 국제해사기구(IMO)에서 선박의 안전운항과 환경보호를 목적으로 결의한 해운회사의 안전경영시스템(Safety Management System)에 관한 국제적 표준규격으로 선박의 물리적 안정성 및 선원의 자질 향상뿐만 아니라 해운기업의 육·해상 모든 부서에서 안전관리시스템을 수립하고 시행하도록 국제해사안전인명협약(SOLAS)의 제9장으로 1994년에 채택된 강제협약임

2) 사이버 위험관리 지원전략 골자 : ① 식별(Identify): 사이버 위험관리에 대한 개인의 역할 및 책임을 정의하고 혼란에 처할 수 있는 선박운용시스템, 자산, 데이터 및 기능 등을 식별 ② 보호(protect): 위험통제 프로세스, 조치 및 비상계획을 수립하여 사이버 사건에 대처하고 해상운송의 연속성 보장 ③ 탐지(Detect): 시기적절하게 사이버 사건을 탐지하는 데 필요한 활동을 개발하고 구현 ④ 대응(Respond): 사이버 사건으로 손상된 해상운송이나 서비스에 필요한 시스템을 복원하기 위한 활동이나 계획을 개발하고 구현 ⑤ 복구(Recover): 사이버 사건으로 손상된 해상운송물류체계 복구를 위하여 필요한 사이버 시스템을 백업하고 복구하기 위한 조치 식별

사이버 위험과 관련된 주요 사건 ^{a)}

■ 지금까지의 사이버 위험은 선박 자체의 탈취보다는 주로 선사의 보안상 취약점을 노려 재정적인 피해를 유발하는 양상을 보임

- 사이버 위험은 자율운항선박(MASS)의 도입과 더불어 단순히 물류시스템을 마비시키는 공격 형태에서 선박 자체를 탈취하려는 시도로 확대될 우려가 있음
- 향후 선박이 육상에서 통제하는 시스템으로 변화된다면 동일한 사양 및 시스템을 가진 다수의 선박에 대해 동시다발적 공격이 가능하여 광범위한 피해를 볼 수 있음

<표 1> 최근 주요 사이버 위험 사건

연번	구분	주요 내용
1	머스크 (A.P. Moller Maersk)	·랜섬웨어(NotPetya) 공격으로 약 3억 달러 손실
2	이란 해운 (Iran Shipping Line)	·사이버 해킹으로 인한 시스템 붕괴 및 선박추적 데이터의 손실 ·선박운영, 재정피해 및 화물손실 발생
3	World Fuel Services	·온라인 뱅킹킹 사기로 약 1,800만 달러 손실
4	리마솔 지역 해운기업	·해커들의 피싱 공격으로 수십만 달러 도난
5	미국 해안경비대	·GPS간섭으로 수 시간 동안 비공개 항만운영이 중단
6	미국 롱비치 항	·여러 건의 대규모 디도스(DDoS) 공격에 노출
7	기타	·중국산 스캐너 장비에 설치되어있던 “좀비 제로(Zombie Zero)”라는 악성코드는 최소 8개 이상의 기업에 침투
8		·마약 밀매업자들은 컨테이너의 이동 및 위치를 제어하는 벨기에 앤트워프 항의 IT 시스템을 파괴하기 위해 해커들을 고용

자료 : A.P. Moller – Maersk improves underlying profit and grows revenue in first half of the year (Maersk, '17), Safety and Shipping Review 2017(AGCS, '17)

정부의 사이버 보안과 관련된 해사안전법 등 관계법령 정비가 필요

■ 사이버보안 관리지침이 포함된 ISM 코드를 반영하여 해사안전법 제46조(안전관리체계)와 제47조(인증심사)에 따라 시행령, 시행규칙의 정비 필요

- 선박의 안전운항관리체계에 사이버보안 내용이 포함될 수 있도록 해사안전법 시행규칙 및 관련 심사규정 등을 개정하여 국내법의 IMO 국제협약 수용 및 이행이 필요함
- 인증심사원이 사이버보안 및 대응에 대한 심사규정과 규정을 이행할 수 있도록, 인증심사원 교육프로그램 개발과 교육 및 훈련을 통한 인증심사원 양성이 필요함

■ 인증심사 업무를 대행하는 기관에서 ISM 인증심사를 수행할 경우, 사이버보안에 대한 심사규정 및 절차를 마련하여 대행 업무를 적절히 수행하도록 조치

- 정부는 기존의 ISM 인증심사 규칙에 사이버보안 및 대응에 관한 ISM 개정내용, ISO/IEC 27001^{b)}, 국제해운회의소(ICS) 등에서 개발한 지침 등을 고려하여 인증심사 매뉴얼 개정 및 보급 업무를 수행해야함
- 정부의 인증심사와 관련하여 대행기관 및 인증심사원, 해운회사를 대상으로 사이버보안 전문교육 수행 및 지원을 위한 계획을 수립해야함

ISM 인증심사 준비 및 사이버보안 취약 분석을 통한 산업계 대응책 마련

■ 산업계는 사이버 공격에 대비한 선박운영체제, 항만물류체계 비상대응 매뉴얼 및 화물손실에 대비한 보상체계 구축 등을 통한 사전대비가 필요함

- 사이버 위협 및 취약성을 해결하기 위한 상세 지침, 국제 및 산업계 표준과 모범사례를 고려하여 회사 자체의 대응 매뉴얼 개발 및 운영이 중요함
- 항만국 통제(PSC)에 대비하여 ISM 매뉴얼에 따른 사이버보안 대응절차 및 시나리오를 개발하여 반영하고, 사이버보안 안전관리체계를 도입하여 선박과 육상에서 운영할 수 있도록 정비하는 것이 필요함

박한선 부연구위원

해운해사연구본부 해사안전연구실
(hspark@kmi.re.kr / 051-797-4627)

참고자료

a) https://www.agcs.allianz.com/assets/PDFs/Reports/AGCS_Safety_Shipping_Review_2017.pdf
(2018.08.16. 검색)

b) https://www.atlaudit.org/uploads/3/9/5/8/39584481/2017_iso-iec_27001_isms_precertification_audit_-_january_2018.pdf (2018.08.17. 검색)