

Vol. 142

2024년 3분기
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 박혜리 실장
- 감 수 이언경 본부장
- 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

해상보안 강화 및 관리를 위한 국제기준 강화 중, 선박, 항만 및 관련시설 간 연결을 위한 사이버보안 협력 필요

■ 제108차 해사안전위원회(MSC), 해상 사이버 위험 관리 지침 개정

➤ 위험 평가 및 사이버 복원력 측면을 강조하는 방향으로 개정

- 해상 사이버 기술은 해사 안전 및 보안, 해양환경의 보호 등을 위해 여러 시스템의 운영 및 관리에 필수적이며 IMO에서는 2017년부터 사이버 위험(Cyber Risk) 관리를 권고함
- 지난 제107차 해사안전위원회(MSC) 회의('23.5.)에서는 MASS 작업반을 통해 네트워크 보안장비 관련하여 MASS Code의 사이버보안, 연결성 개발에 참고하는 것으로 결정(MSC 107/5/INF.11)
- 사이버 보안은 선박뿐 아니라 항만 시설을 대상으로 증가 되는 사이버 공격에도 필수적이며, 디지털화 및 연결성 증가는 사이버 위험에 대한 해사 산업의 취약성 증가로 이어진다는 우려가 제기됨
- 따라서 MSC 제107차 회의에서 해상 사이버 위험 관리 지침 (MSC-FAL.1/Circ.3/Rev.2) 및 해상 사이버 보안 강화를 위한 다음 단계 식별을 향후 이행 의제의 새로운 안건으로 포함하기로 합의함
- 제108차 해사안전위원회(MSC) 회의('24.5.)에서는 문서 MSC 108/6(Australia et al.)를 기반으로 지침에서 기술한 개정안과 IMO 웹사이트 "해상 사이버 위험" 항목에 포함할 해상 사이버 위험 관리 문서에 대한 제안을 고려하도록 요청함
- 이와 함께 MSC 108/6/1(IACS)은 위원회에 문서 부록에 명시된 지침에 대한 제안된 개정안을 검토할 것을 요청했으며, 위험 평가 및 사이버 복원력 측면을 강조함
- 덴마크 등은 문서 MSC 108/6 및 MSC 108/6/1를 기반으로 해상 사이버 위험 관리 지침 (MSC-FAL.1/Circ.3/Rev.2)에 대한 개정안의 통합 초안을 작성하고 사무국에 초안 작성 그룹이 구성될 경우 검토를 위해 논문으로 출판할 것을 요청함

➤ 특히, 디지털 기술 활용에 따른 사이버보안 인식 강화 및 훈련 확대 필요성 제기

- 또한 MSC 제108차 회의에서 디지털 기술은 선박의 운항, 안전 및 보안, 환경 보호 및 연속성에 매우 중요하며, 새로운 위협을 감안할 때 기존 표준을 기반으로 지침을 검토해야 함과 개정된 지침에 비상 상황에 대비한 훈련이 포함되어야 한다는 의견이 제시됨
- 추가로 모든 선원에게 기본적인 사이버보안 인식 교육을 제공해야 하며, 선장에게는 관련 고급 교육을 제공하고 교육 프로그램에는 보고 절차와 훈련 내용이 포함되어야 함이 논의됨
- MSC 제108차 회의에서 위원회는 2017년 해상 사이버 위험 관리 지침(MSC-FAL/Circ.3/Rev.2)에 대한 개정안과 관련 문서 (MSC 108/6, MSC 108/6/1)를 검토 후 개정안을 승인하고, 공동 승인을 위하

- 여 제49차 해상교통간소화위원회(FAL, Facilitation Committee) ('25.3)로 이관함
- 공동 승인이 완료 된 후 개정 초안(MSC-FAL/Circ.3/Rev.3)으로 최종 회람됨
 - 개정된 지침은 위험 평가의 측면을 구체화하고 사이버 위험 관리의 구성 요소를 강화하며 현재 및 향후 사이버 위협과 취약성으로부터 선박을 보호하기 위하여 해상 사이버 위험 관리에 대한 높은 수준의 최신 권고 사항을 제공함
 - 권고 사항으로는 사이버 보안 관련 문서를 그 성격에 맞게 표준(standards), 지침(guidelines) 및 업계 모범 사례(industry best practices)로 구분하여 권고함

▶ 해상 사이버 보안 강화를 위한 관리(Govern) 요소 추가

- 주요 정의, 배경 정보 및 적용과 효과적인 사이버 위험 관리 지원을 강화하기 위해 기존 5가지 기능적 요소에 관리(Govern) 기능을 추가하고, 사용자의 이해를 돕기 위해 각 요소의 의미를 더욱 상세히 설명하고 기타 국제 및 업계 표준, 모범사례와 관련된 내용을 업데이트함
- 총 6가지 기능적 요소로는 관리(Govern), 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)가 있음
- 관리(Govern) 요소는 위험관리 및 정책을 수립하고 모니터링 하며 사이버 위험 관리를 위한 인사 역할 및 책임을 정의함
- 또한 사이버 보안 활동의 계획 및 실행을 담당하는 사람 지정과 백업 관리, 복구 등의 시스템 관리뿐만 아니라 지정된 사람에게 권한과 지원을 제공하는 등 전문성을 갖추도록 함
- 선박의 사이버 복원력을 보장하기 위하여 장비와 시스템을 국제 표준에 따라 설계하고 시험해야 함을 명시함

■ 해상 사이버 위험관리 및 보안 강화 필요성 점차 확대·강화 중

▶ 효과적인 사이버 위험관리를 지원하기 위한 IMO의 사이버 위험관리 지침

- IMO는 사이버 위험 취약성에 대한 상황을 인지하고 제98차 해사안전위원회(MSC) ('17. 6. 7~16) 및 제41차 간소화위원회(FAL) ('17. 4. 4~7)에서 '해상 사이버 위험관리 지침(Guidelines on maritime cyber risk management)¹⁾'을 승인함
- 2017년 6월에 채택된 '해상 사이버 위험관리 지침'의 부속서-10²⁾은 '안전관리시스템 해상 사이버 위험

1) Guidelines on maritime cyber risk management, IMO MSC-FAL.1/Circ.3 (2017. 7. 5)

2) Maritime cyber risk management in safety management systems, IMO Resolution MSC.428(98) (2017. 6. 16)

관리(Maritime cyber risk management in safety management systems)’에 대한 결의안으로 선박 안전관리시스템에 사이버 위험관리 증서가 포함³⁾되도록 함

- 안전관리시스템(Safety Management Systems)은 국제안전관리규약(ISM Code, International Safety Management Code, IMO A.647(16) (1989))의 목적 및 기능 요건에 따라 의무적으로 사이버 위험관리를 수행하고 있음
- IMO의 ‘해상 사이버 위험관리 지침’은 사이버 위협으로부터 효과적인 사이버 위험관리를 지원하기 위한 상위 수준의 기능적 요소를 포함하고 있음
- 선박 시스템에서 사이버 위험에 노출될 수 있는 취약 시스템에는 선교 시스템, 화물 처리 및 관리 시스템, 추진 및 파워 컨트롤 시스템, 접근 제어 시스템, 여객 서비스 및 관리 시스템, 여객 접속 공용 네트워크, 선원 지원 시스템, 통신 시스템이 포함됨
- 선박 시스템에 대한 사이버 위험은 정보와 관련된 IT(Information Technology) 시스템과 운영 기술과 관련된 OT(Operational Technology) 시스템으로 구분하여 관리되어야 함
- 사이버 위험관리는 위험에 대한 식별, 분석, 평가 및 전달하고 이해 당사자에게 취해진 조치의 비용편익을 고려하여 수용, 회피, 이전 또는 완화하는 일련의 과정을 포함함
- 해당 지침은 효과적인 사이버 위험관리 지원을 위한 기능적 요소를 제시하고 있으며, 이러한 기능적 요소는 위험관리 프레임워크에 적절히 통합되어야 함
- 사이버 위험관리 프레임워크는 식별-보호-탐지-대응-복구 절차로 이루어지며, 각각의 절차는 다음 표와 같음

〈표 1〉 해상 사이버 위험관리 프레임워크(IMO)

절차	기능
식별 (Identify)	사이버 위험관리를 위한 인력 및 책임을 정의하고 시스템, 사이버 자산, 데이터 및 기능을 식별
보호 (Protection)	사이버 공격으로부터 보호 및 선박 운용을 보장하기 위한 위험통제 프로세스, 조치 및 비상계획을 수행
탐지 (Detection)	사이버 공격을 적시에 탐지하기 위한 기능 개발 및 구현
대응 (Respond)	사이버 공격으로 인해 손상된 서비스 및 선박 운용에 필요한 시스템 복구를 위한 기능 개발 및 구현
복구 (Recover)	사이버 공격으로 영향을 받는 선박 운용에 필요한 시스템의 복구, 백업 기능 개발 및 구현

자료 : Guidelines on maritime cyber risk management, IMO MSC-FAL.1/Circ.3 (2017. 7. 5)

3) 기국으로 하여금 2021년 1월 이후 도래하는 첫 번째 연차검사에서 사이버 위험에 대한 관리가 안전관리시스템 안전관리시스템은 국제안전관리규약(ISM Code, International Safety Management Code, IMO A.647(16) (1989))의 목적 및 기능 요건에 따라 사이버 위험관리 수행에서 수행되고 있음을 나타내는 적합증서(DoC, Document of Compliance)를 비치하도록 권고함

▶ 산업계 및 국제표준으로 적용되는 해상 사이버 위험관리 지침의 모범사례 제공

- 선박 사이버 보안 지침(The Guidelines on Cyber Security Onboard Ships)은 선주단체(BIMCO, INTERCARGO, InterManager, INTERTANKO, ICS, IUMI, OCIMF 등)에서 제작하였음
- 해당 지침은 선원, 환경, 화물 및 선박의 안전과 보안을 개선하기 위해 작업 프로세스, 장비, 교육, 사고 대응 및 복구 관리에 중점을 두고 선박 내 관련 규정과 모범사례에 따라 적절한 사이버 위험 관리 전략을 개발하는 데 도움을 주는 것을 목표로 하고 있음
- ISO/IEC 27001 표준(Standard)은 ISO와 IEC에 의해 공동 발행되었으며, 정보기술(Information technology) - 보안기술(Security techniques) - 정보보안 관리시스템(Information security management systems) - 요구사항(Requirements)에 관한 내용을 포함하고 있음
- 미국 NIST 사이버보안 프레임워크(National Institute of Standards and Technology Cybersecurity Framework)는 미국의 주요 사회기반시설에 대한 사이버 공격 시도가 국가 경제와 안보에 미칠 위협에 대비하기 위해 개발 되었음
- 이 프레임워크는 코어, 프로필, 구현 계층의 세 부분으로 구성되고 비즈니스 관점에서 사이버보안 활동을 계획하고 조직의 위험관리 프로세스의 일부로 사이버보안 위험을 고려하고 있음

■ 2024 한국해사주간 기간 중, 제3차 해사 사이버안전 전문가 포럼 개최

- ▶ 2024 한국해사주간에서는 국제해사분야에서 가장 큰 이슈인 탈탄소화(Decarbonization)와 디지털화(Digitalization)에 대응하기 위한 해사산업 미래전략에 대해 논의
 - 2024 한국해사주간(2024 Korea Maritime Week)이 9월 9일(월)부터 12일(목)까지 4일간 부산에서 ‘국제 해운분야 대전환 시대, 도전과 기회’라는 대주제로 개최됨
 - 해양수산부 강도형 장관, IMO 아르세뇨 도밍게스 사무총장, 임기택 명예사무 총장, 한국해양수산개발원 김종덕 원장, 한국해양대학교 류동근 총장 등을 비롯해 국내외 관련 분야 전문가 다수가 참석함
 - 행사 첫째 날에는 개회식과 더불어 ‘국제 해운의 탈탄소화 및 디지털화에 따른 국제사회의 노력과 과제’를 주제로 국내외 주요 인사들이 참여하는 고위급 대담이 개최되었고 둘째 날부터는 첨단 해양모빌리티 기술과 정책을 토론하는 15개의 행사가 진행됨⁴⁾
 - 해양수산부 강도형 장관은 “한국해사주간은 해운, 조선, 항만 등 선박이 관련된 다양한 분야의 최신 기술 동향과 정책 방향을 공유하고 주요 국가들과 협력 방안이 논의되는 국제협력의 장이다.”라며, “이번 한국

4) ‘글로벌 첨단 해양모빌리티 포럼’, 해양 디지털화를 주제로 한 ‘아·태지역 해양디지털 국제 콘퍼런스’, 녹색해운항로, 친환경 전략 등을 논의하는 ‘해운탈탄소 포럼’, 사이버안전 국제 동향을 논의하는 ‘해사 사이버안전 전문가 포럼’, 해양안전과 해양 모빌리티 기술을 홍보·전시하는 ‘해양모빌리티 안전엑스포’ 등

해사주간을 통해 국제사회가 해사분야의 핵심의제에 대한 동향을 상호 공유하고 미래 발전 방안을 함께 모색해 나갈 수 있기를 기대한다.”라고 언급함

▶ 제3차 해사 사이버안전 전문가 포럼, 사이버안전 국제 동향을 논의

- 제3차 해사 사이버안전 전문가 포럼이 2024 한국해사주간의 일환으로 9월 11일(수)에 파라다이스호텔 부산에서 개최됨
- 해사 사이버안전 전문가 포럼은 2022년부터 매년 개최 중인 행사로, 이번 행사는 해양수산부 최성용 해사 안전국장, 이창용 해사안전정책과장 등을 비롯해 국내외 해사 사이버안전 관련 전문가 다수가 참석함
- 해양수산부는 해사 사이버안전 관련 국제동향과 정책 추진 현황을 공유하였고 인터넷진흥원과 울산과학기술원에서는 스마트선박 보안 기반 사업 및 보안기술 등을 소개함
- 또한 Maersk사에서는 자사의 랜섬웨어 피해·대응 사례 소개를 통해 사이버 복원력의 중요성에 대해 발표했고 학계에서는 SI기반 네트워크 보안 장비 및 항만 스마트화에 따른 네트워크 구조 분석과 사이버 보안 가이드라인 등을 발표하였음
- 실제 피해사례와 국제동향 소개 등을 통해 사이버안전 관리의 필요성에 대한 강조와 관련 기술 동향에 대한 논의로 사이버안전 중요성에 대한 공감대가 형성됨

〈그림 11〉 2024 한국해사주간 개막식



자료 : 해양수산부

국제사회에서의 해상 사이버 보안 관련 최근 논의사항

▶ 국제항로표지협회(IALA) 자체 사이버보안 가이드라인 개발 중

- IALA 이네비위원회(ENAV, ENAVigation Committee) 제24차 회의('19.10.)에는 IEC 62443⁵⁾ 및 IEC 61162-460⁶⁾ 표준에 기초한 해상 ICT 장비에 적용되는 사이버보안 형식승인 사례와 적용 사례를 소개한 의제문서(Introduction of cyber security type approval applicable case based on IEC 62443 and IEC 61162-460 standards)⁷⁾가 제출됨
- 이는 IEC 62443 표준, 산업자동화제어시스템(IACS, Industrial Automation and Control System) 구성요소의 기술 보안 요건 및 적용 사례에 따라 IALA에 사이버보안 형식 승인 사례를 제공하기 위한 정보 문서임
- IALA ENAV 제27차 회의('21.3.)에는 '자율운항선박 개발 가이드라인(IALA guideline on developments in Maritime Autonomous Surface Ships)⁸⁾' 초안이 제출되었으며, MASS 환경을 지원하기 위한 가이드선스(guidance) 개발 우선순위 항목을 식별함
- IALA ENAV 제27차의 '자율운항선박 개발 가이드라인' 초안문서에서 식별된 가이드선스 개발 우선순위는 다음과 같음
 1. 고정식 해안 AtoN 시스템(Fixed shore side AtoN)
 2. 부표식 AtoN 시스템(Floating AtoN)
 3. 가상 AtoN(Virtual AtoN)
 4. 합성 AtoN을 이용한 물리적 AtoN 표식(Marking of physical AtoN using Synthetic AtoN)
 5. ASM(Application Specific Messages)을 이용한 기상 및 수로 데이터 전송(The transmission of local and applicable Meteorological and Hydrographic data using Application Specific Messages (ASM) contained in IMO Circular SN.1/289)
 6. VTS 구역내 선박간 통신 보장 및 다양한 자율수준 인식(Supporting the safe and efficient operations within a VTS environment)
 7. VTS 구역내 항로상 상황인식을 위한 공동운용개념 공유(Ensuring communication between

5) Security for industrial automation and control systems, IEC 62443:2019 (2019)

6) Maritime navigation and radiocommunication equipment and systems - Digital interfaces, IEC 61162-460:2018 (2018)

7) Introduction of cyber security type approval applicable case based on IEC 62443 and IEC 61162-460 standards, IALA ENAV24-6.1.14 (2019. 10)

8) IALA guideline on developments in Maritime Autonomous Surface Ships, IALA ENAV27-12.2.2 (2021. 03)

vessels within a Vessel Traffic Service (VTS) environment, recognising the different degrees or levels of autonomy)

8. MASS 육상센터(SCC, Shore Control Center) 및 VTS 센터간 상호작용 범위에 대한 지침 개발 (Sharing of a common operating picture for situational awareness of the waterway within Vessel Traffic Services (VTS) environment)
 9. 선박교통 이미지 지원을 위한 MASS 선박 및 기존선박의 추적(Scoping and development of guidance on the interaction between VTS and the control centre for MASS(Shore Control Centre, SCC))
 10. 선박교통 이미지 지원을 위한 MASS 및 non-MASS 선박 트래킹(The tracking of both MASS and non-MASS vessels to support the traffic image)
 11. 사이버보안 - 사이버 위험관리(Cyber Security - cyber risk management)
 12. 측위시스템 보강(Augmentation of positioning systems)
 13. 표준화된 데이터 전송 촉진(Promoting standardization of data transfer)
- IALA ENAV 제28차 회의('21.10.)에는 '국제표준 기반 선박 e-Navigation 서비스 표시장치에 적용 가능한 사이버보안 요구사항(The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards)⁹⁾ 의제문서가 제출됨. 선박의 e-Navigation 서비스 장치에 사이버보안 요구사항을 도출하기 위해 수행된 정보가 포함되어 있음
 - IALA는 사이버보안 워크숍을 개최하고 IALA의 사이버보안 논의 방향을 결정하였는데 항로표지, VTS 등 항행지원시설에 대한 사이버보안의 인적요소를 절차로 해서 기술에서는 IALA 범위 내 플랫폼, 하위 시스템 그리고 사고복구에서는 사이버 사고 대응 및 복구에 대해 논의가 되었음
 - 사이버보안 절차 고려 시, 항로표지 및 VTS에 대한 인적요소 고려가 필요한데 그 권고사항으로는 "사이버 보안과 관련된 인식을 높이고 사이버보안에 대한 정기적인 교육 제공 필수, 사이버 보안 관련 역할 및 책임이 조직 전체 차원에서 진행 및 할당, 사이버 보안에 관한 인식은 조직 전반에 필요, 사이버 보안은 시스템의 수명 주기 관리에 포함되어야 함"이 있음
 - 사이버보안 위험 취약 시스템 식별, IALA 작업 범위 내에서 사이버보안을 다루기 위한 추가 작업 제안으로 "GNSS 신뢰성 확보 필요 (ENG WG3, ENAV WG2 작업 지원), 식별된 사이버 위험으로부터 IT를 보호 중요성 강조, VTS운영 시 AIS와 GNSS에 대한 사이버 보안 위험으로부터 보호 방법 강구, AIS 메시지 인증에 대한 장기적인 해결책 마련 필요, 저대역폭 응용프로그램에서 PKI 사용을 지원하는 암호화 솔루션 마련 (ENAV WG1), IEC 63173-2 SECOM(S-100) / IP기반 통신 지원 업데이트를 위해 검토 필요"가 권고됨

9) The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards, IALA ENAV28-5.1.1.4 (2021. 03)

- 사이버보안 관련 사고 후 대응 및 복구 방안 마련으로 “사이버보안 위험은 기존 비즈니스 연속성 계획에 포함, AtoN 및 OT 시스템에 대한 사고 시나리오 개발 필요, 업무 연속성은 조직 전체에 할당, 모범사례 필요, 사이버 사고 정보의 보고 및 공유수단 필요”가 권고됨
- 워크숍의 주요 결론은 다음과 같음
 - 사이버 보안 위험은 조직 전반에 걸쳐 이해되어야 함
 - VTS, 항로표지는 중요한 인프라이며, 보안에 대해서는 표준적용이 필요함
 - PNT, AIS는 보안에 취약함
 - VTS의 연속적인 운영을 위해서는 사이버보안이 고려되어야 함 (계획 수립)
 - 레거시 시스템은 여전히 사용하고 있지만 적절한 백업 생성 필요
 - 사이버 보안에 대한 역할 & 책임 할당 필요
 - 사이버 보안은 시스템의 수명 주기 관리에 포함되어야 함
 - ARM 위원회는 사이버 보안 하도록 IALA Risk toolbox 변경 검토
 - 사고 복구를 위한 VTS, 항로표지 시나리오 개발
 - 사고 대응을 위한 명확한 계획 및 정책 수립 필요
 - 사이버 사고의 최초 대응은 항로표지, VTS 제공자이며, 추가 분석을 위한 제3자 전문가가 필요함
 - 항로표지 사이버 보안 사고는 이해 관계자에게 보고되고 공유되어야 함
 - 항로표지, VTS 시스템 운영 조직 내에서 사고 대응 및 위기 관리자에 대한 교육이 필요함
- 워크숍의 주요 결론을 바탕으로 IALA 자체 사이버보안 가이드라인을 개발 중이며 사이버보안과 관한 기존 표준이나 모범사례에서 다뤄지지 않은 IALA 관련 주체에 대한 사이버보안 가이드라인을 제시함

➤ ISO 및 IEC, “정보기술-보안기술-정보보안 관리시스템-요구사항”에 대한 표준 마련(ISO/IEC 27001)

- 국제표준화기구(ISO, International Organization for Standardization) 및 국제전기기술위원회(IEC, International Electrotechnical Commission)의 ISO/IEC 27001은 정보보안 관리체계에 대한 국제표준으로 2005년 ISO와 IEC에 의해 공동 발행되었으며, IMO의 ‘해상 사이버 위험관리 지침’에 모범사례로 포함되어 있음
- 해당 표준은 조직의 상황(조직에 대한 이해, 이해관계자의 기대 및 요구사항 이해, 정보보안 관리시스템의 범위), 지도부(지도부의 책무, 정책, 역할 및 책임), 책임(위험조치 - 정보보안 위험 평가/ 정보보안 위험 취급¹⁰⁾, 정보보안대상 및 계획), 정보보안 관리체계 지원 및 운영, 성능 평가, 개선 등의 내용으로 구성됨

10) ISO/IEC 27001 6.1.3절 - 정보보안 위험 취급(Information security risk treatment), ISO/IEC 27001 (2013. 10.01)

- 해당 표준의 부속서¹¹⁾에는 정보보안 위험 취급을 위한 위험관리 통제대상 및 통제항목을 제시하고 있으며, 통제 대상에는 다음의 사항이 포함되어 있음

- A.5 : 정보보안 정책
- A.6 : 정보보안 조직
- A.7 : 인적 보안
- A.8 : 자산 관리
- A.9 : 접근 통제
- A.10 : 암호화 정책
- A.11 : 물리적 · 환경적 보안
- A.12 : 운영 보안
- A.13 : 통신 보안
- A.14 : 시스템 획득, 개발 및 유지관리
- A.15 : 공급자 관계
- A.16 : 정보보안 사고 관리
- A.17 : 비즈니스 연속성 관리의 정보보안 측면
- A.18 : 준수

➤ 국제선급협회(IACS), 사이버복원력을 위한 공통규칙을 2024년 7월 1일 이후 건조계약 되는 선박에 적용

- 국제선급협회는 선박에 대한 해킹 및 랜섬웨어 등 사이버 위협 증가에 따른 선박의 사이버 복원력 강화를 위해 선박의 사이버복원력을 위한 공통규칙을 발표함
- 공통규칙에는 UR E26 Cyber resilience of ships(선박의 사이버 복원력)과 UR E27 Cyber resilience of on-board systems and equipment(온보드 시스템 및 장비의 사이버 복원력)가 있음
- 두 규칙은 2024년 1월 1일 이후 건조계약을 체결한 신규 선박에 적용 예정이었으나 사이버 보안 경험을 반영하는 업계 피드백에 따른 개선 사항으로 인해 2024년 7월 1일 이후 건조계약 되는 선박에 적용됨
- IACS 사무총장인 로버트 애시다운은 “IACS 요구사항이 적용 가능성에 대해 명확하고 선박 조사에서 일 관되게 적용될 수 있도록 업계 피드백을 통합하는 것은 사이버 복원력을 강화하기 위한 조치에 영향을 미 치므로 중요하며, 결과적으로 기존 요구사항이 아직 발효되지 않았다는 점을 감안하여 IACS는 2024년 7

11) ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001 (2013. 10. 01)

월 1일부터 개정된 요구사항만 적용 하기로 결정했고 업계는 이 결정이 가져오는 정확성으로 인해 환영할 것으로 믿는다”라고 언급함

- 선박에서 발생하는 사이버 사고가 인명, 재산 및 환경에 직접적인 악영향을 미칠수 있음을 인식하고 선박 Onboard 컴퓨터 기반 시스템의 신뢰성과 기능적 효율성에 대해 꾸준히 주목함
- 사이버 시스템 공동작업그룹을 소집하여 접근방식 등을 식별 및 공통규칙 발표는 연결성이 가속화되는 디지털 해양 세계에 대한 국제선급협회의 중요한 이정표로 의미가 있음
- UR E26은 선박의 설계, 건조, 시운전, 운항까지 선박의 운용주기 동안 운영기술(OT) 및 정보기술(IT) 장비를 선박 네트워크에 안전하게 통합하는 것을 목표로 함
- 또한 사이버 복원력을 위한 집합체로 선박을 대상으로 하며, 장비 식별, 보호, 공격탐지, 대응 및 복구의 5가지 주요 측면을 다룸

〈표 2〉 UR E26의 주요내용

목차	주요내용
도입	개요
	정의
	목적 및 조직의 요구사항
본문	<p>요구사항</p> <ul style="list-style-type: none"> - 식별 (Identify) : 선상 시스템, 사람, 자산, 데이터 및 기능 사이버 위험을 관리하기 위한 조직적 이해를 개발 - 보호 (Protect): 사이버 사고로부터 선박을 보호하고 운송 연속성을 극대화하기 위한 적절한 보호 장치 개발 및 구현 - 탐지 (Detect) : 선상에서 사이버 사고의 발생을 탐지하고 식별하기 위한 적절한 조치를 개발하고 구현 - 대응 (Respond) : 선내에서 탐지된 사이버 사고에 대해 조치를 취하기 위한 적절한 활동 개발 및 구현 - 복구 (Recover) : 사이버 사고로 인해 손상된 운송에 필요한 모든 기능 또는 서비스를 복구하기 위한 적절한 조치 및 활동을 개발하고 구현
	<p>성능시험을 위한 시험계획</p> <ul style="list-style-type: none"> - 설계 및 건조 단계 - 시운전 단계 - 선박 운용 단계
보충	요구사항에서 CBS 제외 시 위험도 평가
	부록 : 조치 및 문서, 요구사항 요약

자료 : Cyber resilience of ships – Rev.1 Nov 2023 – Complete Revision, IACS

- UR E27은 제조사 및 기자재 시스템 요구사항으로 시스템 무결성이 제조사에 의해 보호되고 강화하는 것을 목표로 함
- 온보드 시스템 및 장비의 사이버 복원력에 대한 요구사항을 제공하고 사용자와 온보드 컴퓨터 기반 시스템 간의 인터페이스와 관련된 추가 요구사항을 제공

〈표 3〉 UR E27의 주요내용

요구사항	참조 표준	카테고리
시스템 기본 요구사항	IEC 62443 3-3[9] SR(System Requirement) 31개 항목	<ul style="list-style-type: none"> - 식별 및 인증 - 사용제어 - 시스템 무결성 - 데이터 기밀성 - 사고에 대한 적시 대응 - 리소스 가용성
시스템 추가 요구사항	IEC 62443 3-3 SR 10개 항목	<ul style="list-style-type: none"> - 식별 및 인증 - 사용제어 - 시스템 무결성
제조사 요구사항	IEC 62443 4-1[10] 7개 항목	<ul style="list-style-type: none"> - 보안 관리 - 보안 업데이트 관리 - 보안 가이드라인

자료 : Cyber resilience of on-board systems and equipment – Rev.1 Sep 2023 Clean, IACS

- UR E26에 정의된 컴퓨터 시스템 기반에 적용되며, 항법 및 무선 통신 시스템은 UR 요구사항 대신 IEC 61162-460을 따를 수 있으며 대상 장비는 다음과 같음
- 네트워크 장비 (라우터, 관리 스위치 등)
- 보안 장치 (방화벽, 침입 방지 시스템 등)
- 컴퓨터(워크스테이션, 서버 등), 자동화 장치

IMO, 해사산업 사이버 보안 강화를 위한 내부자 위협 툴킷 출시

- ▶ 2024년 8월, IMO는 글로벌 해사산업의 끊임없이 진화하는 내부자 위협(Insider Threat) 대응을 위한 새로운 툴킷(Toolkit) 출시
 - 내부자(Insider)란 보안 위치, 품목 또는 민감한 정보에 대해 접근과 지식 등을 제공하는 해상 부문(해운, 항만 및 기타 관계자 포함) 또는 관련 업계에 일하는 직원을 말함
 - 툴킷(Toolkit)은 특정 작업이나 목표를 달성하기 위해 필요한 도구 모음을 의미하며 특정 문제를 해결하거나 프로젝트를 진행하는 데 필요한 지침, 템플릿, 자료 등을 포함함
 - 내부자 위협이란 해사산업 직원의 인식 부족, 무지 또는 악의적인 행동 등으로 보안 사고를 저지르거나 가능하게 함으로써 발생하는 위험을 말함
 - 테러리스트, 조직 범죄 집단 등은 보안 제어의 취약성을 악용하고 해운 및 항만 부문 전체에 사이버 보안 사고를 지속적으로 일으키고 있고 이러한 사고는 내부자를 악용하여 촉진 될 위험이 있음
 - 이러한 문제를 해결하기 위해 IMO는 국제민간항공기구(ICAO)와 협력하여 교육 목적으로 새로운 내부자 위협 툴킷을 개발함
 - 해사 행정부, 지정 기관, 선박 회사, 항만 운영자 및 기타 관계자를 포함하여 해양환경에서 운영되는 조직이 끊임없이 발생하는 내부자 위협에 더 잘 대응할 수 있도록 설계함
 - 협력하여 개발 된 툴킷은 백그라운드 검사 및 심사, 접근 제어 조치, 순찰, 감시 및 모니터링, 침단 기술 및 인공 지능 사용을 포함한 다양한 모범사례 보안 조치를 설명함
- ▶ 해상 사이버 위험에 대한 'One-UN' 접근 방식이 중요함을 강조
 - 현재 전 세계적으로 매우 다양한 해상 사이버 위험에 직면해 있기 때문에 파트너 UN기구와 기관을 포함하는 'One-UN' 접근 방식이 중요하며 새로운 제품과 교육 개발 및 해상 보안 조치를 이행하려는 회원국을 지원하는 것이 필수적임
 - IMO는 해당 툴킷을 국제적 해사 관련 기관과 선박 회사 및 기타 관계자들을 포함한 모든 조직에서 사용할 수 있도록 지원함

〈그림 12〉 Insider Threat Toolkit



자료 : IMO

■ 사이버 보안 위험사고 증가에 따른 국제적·일관적 사이버 보안 체계 필요

▶ 해양 장비의 디지털화 등으로 해상 사이버 보안 위험사고 증가 중

- IMO에서는 디지털화 및 연결성 증가에 따라 사이버 보안 위험사고 증가를 우려하고 있음
- 디지털화 및 연결성 증가에 따른 사이버 기술은 앞으로 더욱 중요한 요소로 사이버 보안은 필수적임
- 이러한 상황이 지속적일 것으로 예상되기 때문에 제107차 MSC에서 기존 해상 사이버 위험 관리 지침 (MSC-FAL.1/Circ.3/Rev.2)의 개정 및 해상 사이버 보안 강화를 논의하였고, 제108차 MSC에서 해상 사이버 위험 관리 지침 개정 초안(MSC-FAL/Circ.3/Rev.3)이 승인됨
- 또한 IALA에서는 연결성 증가에 따른 표준적용 필요로 자체 사이버보안 가이드라인 개발 중이며 IACS에서는 위험사고 증가에 따라 사이버 복원력을 위한 공통규칙을 2024년 7월 1일부터 적용함

▶ 선박의 디지털화 및 첨단화에 따른 해상 사이버 위협으로부터 보안 필요

- 제48차 FAL 회의('24.4.)에서 2024년 1월부터 의무화된 항만의 해상싱글윈도우(Maritime Single Window, MSW)서비스 지침을 최신화함
- 해상싱글윈도우란 선박의 항만 입출항 등에 필요한 공적문서(행정정보)를 표준화 및 싱글윈도우를 통한 전자 제출 지원 시스템을 말함
- 해상싱글윈도우의 의무화에 따라 사이버 위협으로부터 안전한 시스템의 구축 필요성이 강조됨
- 제11차 항해통신·수색구조전문위원회(NCSR, Sub-Committee on Navigation, Communication and Search and Rescue) 회의에서 2029년 1월 이전 전자해도표시시스템(Electronic Chart Display and Information System, ECDIS¹²⁾) 설치 선박 대상으로 전자 항해용 문서(Electronic Nautical Publication, ENP¹³⁾) 관리지침 개발 필요성에 대해 논의됨
- MSC 제108차에서 선박의 디지털화로 인한 사이버 위협으로부터 보안 필요성 제기와 MASS Code 개발 로드맵 등 자율운항선박에 관한 IMO 중장기 작업 계획이 수정 및 구체화 됨

▶ 사이버 안전을 확보할 국제적 해상 사이버 보안 표준 필요

- 국내에서는 이러한 대응의 일환으로 2022년부터 지금까지 해사 사이버안전 전문가 포럼을 개최해 오고 있으며 관련 국제 기술 동향에 대해 논의하며 사이버 보안에 대한 중요성을 알리고 있음
- 특히 이에 대응하기 위한 협의체 및 관련 정책과 규정을 만들고 다양한 국가와 협력 및 소통이 필요함
- 사이버 보안 규정은 관할권 내에서 일관되지 않으며 국제적으로 운영되는 선박 및 항만 시설에 대해 표준화가 되어있지 않아 지역에 따라 보안 수준이 달라짐
- 이러한 문제를 해결하기 위해 전 세계 해양산업 전반에 통용되는 공통적인 해상 사이버 보안 표준이 필요하며 또한 이를 위해서는 전 세계의 네트워크 구축과 협력적 접근 방식이 마련되어야 함

▶ 동시에 항만 시설과 상호연결 되는 일관적인 사이버 보안 체계 마련 필요

- 현재까지 사이버 보안에 대한 IMO의 주요 초점은 선박에 맞춰져 있었지만 항만 시설 또한 사이버 공격에 노출 되어있기 때문에 관심이 필요함
- 항만은 해운과 내륙교통을 연결하여 물류 활동이 이루어지는 국제적인 연결지점으로 사이버 보안 위협사고가 일어날 시 물류시스템에 큰 위협을 줄 수 있음

12) 전자해도표시시스템(Electronic Chart Display and Information System, ECDIS) : 선박의 항해와 관련된 정보, 즉 해도정보, 위치정보, 선박의 침로, 속력 등을 종합하여 컴퓨터 스크린에 도식하는 시스템을 말하며 국제해사기구(IMO)와 국제수로기구(IHO)에 의해 정해진 표준사양서(S-52)에 따라 제작된 것만을 전자해도표시시스템이라 함

13) 전자 항해용 간행물(Electronic Nautical Publication, ENP) : 종이 항해용 간행물을 대신하여 조석표 등대표 해상 기상정보 항만 정보 등을 전자 형태로 제공

- 일부 IMO 회원국에서는 이러한 문제를 인식하고 새로운 사이버 보안 지침 관련 의견을 제시함
- 해양 인프라는 광범위하며 여러 부문이 상호연결 되어있기 때문에 서로 큰 영향을 미칠 수 있음
- 따라서 기존의 선박 위주 사이버 보안 체계에서 항만 시설과 상호연결 되는 일관적인 사이버 보안 체계 마련이 필요함

박제영 연구원

물류·해사산업연구본부 해사산업·안전연구실
(jetyranno@kmi.re.kr / 051-797-4589)

참고
자료

- a) IACS(2023), Guidelines for Cyber resilience of on-board systems and equipment
- b) IACS(2024), Guidelines for Cyber resilience of ships
- c) IALA(2019), ENAV24-6.1.14, Introduction of cyber security type approval applicable case based on IEC 62443 and IEC 61162-460 standards
- d) IALA(2021), ENAV27-12.2.2, IALA guideline on developments in Maritime Autonomous Surface Ships
- e) IALA(2021), ENAV28-5.1.1.4, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards
- f) IEC(2018), 61162-460, Maritime navigation and radiocommunication equipment and systems – Digital interfaces
- g) IEC(2019), 62443, Security for industrial automation and control systems
- h) IMO(2017), MSC-FAL.1/Circ.3, Guidelines on maritime cyber risk management
- i) IMO(2017), Resolution MSC.428(98), Maritime cyber risk management in safety management system
- j) IMO(2019), MSC 101/5/5, Draft interim guidelines for MASS trial
- k) IMO(2022), MSC-FAL.1/Circ.3/Rev.2, GUIDELINES ON MARITIME CYBER RISK MANAGEMENT
- l) IMO(2024), MSC 108/WP.1, DRAFT REPORT OF THE MARITIME SAFETY COMMITTEE ON ITS 108TH SESSION
- m) ISO/IEC(2013), ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements
- n) <https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release> (검색일: 2024.09.20.)
- o) <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> (검색일: 2024.09.18.)
- p) <https://www.imo.org/en/MediaCentre/Pages/WhatsNew-2116.aspx> (검색일: 2024.09.20.)
- q) <https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=971&bbsSeq=10&docSeq=58410> (검색일: 2024.09.02.)
- r) <https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=971&bbsSeq=10&docSeq=58599> (검색일: 2024.09.13)
- s) <https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=381&bbsSeq=15&docSeq=58687> (검색일: 2024.09.16)