2020 제 5 호

최신외국법제정보

Issue Brief on Foreign Laws

맞춤형 법제정보

중 국 낚시어선업법제

스웨덴 기업활력법제

외국법제동향

미 국 가상화폐세법

미 국 「공정주택법」

일 본 임대용 주택관리법제

독 일 암호화폐 수탁업법제

중 국 「암호법」

국제기구 해상 사이버 리스크 규범

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

KOREA
LEGISLATION
RESEARCH INSTITUTE

최신외국법제정보

Issue Brief on Foreign Laws

KLRI

해상 사이버 리스크 관리를 위한 국제적 동향

- 국제해사기구, 발틱국제해운동맹, 국제선급연합회를 중심으로 -

이현균 | 고려대학교 법학전문대학원 연구교수, 법학박사

Ⅰ. 들어가며

4차 산업혁명으로 불리는 최근의 과학기술 발달은 해운산업에도 영향을 미쳐 이른바 자율운항선박이 머지 않아 상용화될 것으로 예상되고 있다. 영국 비영리 해양연구기관 프로메어(Promoting Marine Research and Exploration, ProMare)와 IBM은 올해 9월 인간의 개입이 전혀 필요 없는 인공지능 기반 완전 자율운항선박인 'Mayflower호'를 완공해 2021년 대서양 횡단 항해를 통해 최종적인 성능시험을 할 계획이라고 발표했다.[1] 우리나라에서도 올해 9월 LIG넥스원이 개발한 '해검 II'의 자율운항 및 원격통제 기술력 평가를 완료했다.[2]

자율운항선박 이전의 기존 선박은 육상에서 떨어져 물리적인 접근이 어려워 전통적인 운용기술(Operational Technology, OT)을 중심으로 운항되기 때문에 항해 중인 선박은 육상으로부터의 고립성, 기술적 제한성 등 육상의 다른 산업분야에 비해 사이버 공격으로부터 비교적 자유로웠다.

운용기술(OT) 시스템은 물리적인 설비와 절차를 직접 모니터하거나 통제하는 하드웨어 혹은 소프트웨어를 말한다. 반면 정보통신기술(IT) 시스템은 정보처리에 관한 다양한 기술 즉, 소프트웨어, 하드웨어, 통신기술 등을 포함한다. 즉, 운용기술(OT) 시스템은 주로 물리적인 환경을 통제하며, 정보통신기술(Information Technology, IT) 시스템은 데이터를 운영한다. 원래 운용기술(OT)은 물리적인 환경을 통제하고 정보통신기술

1 윤영주, "AI 메이플라워호 출항 준비 끝...내년 초 英 플리머스항 출발", AI타임즈, 2020. 9. 17, http://www.aitimes.com/news/articleView.html?idxno=132285.

2 김동민, "경남도, 해검 II 운항 등 '무인선박' 실증 성공", 연합뉴스, 2020. 9. 23, https://www.yna.co.kr/view/AKR20200923140900052?input=1195m.

(IT)은 데이터를 운영하는 구분되는 개념이었으나, 〈그림-1〉에서 보는 바와 같이 선박에서 해상연결성기술, 제어기술 등 해상위성통신시스템 등의 활용도가 높아지면서 개별적으로 운영되던 운용기술(OT)과 정보통신기술(IT)은 통합되어 점차 그 경계가 모호해지고 있다.[3)]

〈그림-1〉 자율운항 선박 기술 개요도[4)]

즉, e-Navigation 도입, 자율운항선박 상용화 등 기술의 발달로 선박에서의 정보통신기술(IT)과 운용기술(OT)이 통합되고 선박이 육상과 인터넷을 통해 연결되면서 해상 사이버 리스크의 중요성이 급속도로 증가하여 선박의 여러 구성요소도 더 이상 사이버 공격에서 자유롭지 못하게 되었다.

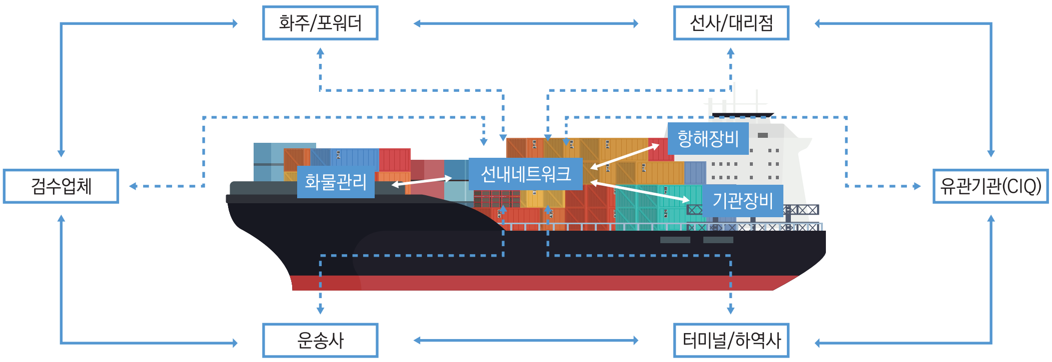
또한 해운을 포함한 물류분야는 그 특성상 선박소유자 등 해운기업은 해상에서 운항중인 개별 선박과의 내부적 운영정보 교환뿐만 아니라, 운송단계별로 화주, 운송인주선인, 항만운영자, 창고관리자, 세관 등 다양한 분야에서 외부적인 의사소통이 필요하다. 〈그림-2〉에서 보는 바와 같이 복잡한 업무 프로세스 속에서 필연적으로

3 BIMCO et al, "The Guidelines on cyber security onboard ships", ver. 3, 2018, p.5.

4 한국정보통신기술협회, ICT 표준화전략맵 ver.2020, 요약보고서, 2019, 146면.

다양한 이해관계자들과의 협력이 필요하므로 사이버 리스크 관리의 영역은 선박 내로 국한되지 않고 물류 전 과정에서 중요하다.[5)]

〈그림-2〉 해운 물류분야 업무 프로세스[6)]



자율운항선박 상용화 등 기술의 발달과 함께 해운 물류분야의 업무 효율성이 크게 증대될 것으로 기대되지만, 사이버 리스크에 대한 대비는 선결적으로 해결해야 할 필수적인 문제이다. 이에 대한 논의를 위해 먼저 해상 사이버 리스크의 정의 규정과 최근 사고 사례를 통해 해상 사이버 리스크의 개념과 현황에 대해 살펴본다.

5 이현균·권오정, "해상사이버리스크에 관한 영국보험업계의 대응과 시사점", 보험법연구 제14권 제2호, 한국보험법학회, 2020, 218면.

6 박한선, 해상 사이버 보안체계 강화방안 연구, 한국해양수산개발원, 2019, 13면.

Ⅱ. 해상 사이버 리스크의 개념과 최근 사고 사례

1. 해상 사이버 리스크의 개념

국제해사기구(International Maritime Organization, IMO)는 해상 사이버 리스크(maritime cyber risk)를 "기술 자산이 잠재적 상황이나 사건에 의해 위협을 받을 수 있는 것으로서, 정보 혹은 시스템이 손상, 손실 혹은 훼손된 결과 그것이 해운과 관련된 사업운영, 안전 혹은 보안의 실패를 초래하는 것"으로 정의한다.[7)]

발틱국제해운동맹(BIMCO)은 사이버 공격(cyber attack)을 "IT 및 OT 시스템, 컴퓨터 장치를 대상으로 회사 및 선박 시스템과 데이터를 손상, 파괴 또는 접근하려는 모든 유형의 공격"으로, 사이버 사고(cyber incident)를 "실제로 또는 잠재적으로 선박의 시스템, 네트워크 및 컴퓨터 또는 정보에 부정적인 결과를 초래될 것이 예상되어 대응 조치가 필요한 상황"으로 각각 정의하고 있다. 그리고 사이버 리스크 관리(cyber risk management)는 "사이버 공격과 사고를 대응해 사이버 관련 위험을 식별, 분석, 평가 및 전달하고, 이해당사자에게 취한 조치의 비용과 편익을 고려하여 이를 수용 가능한 수준으로 수용, 회피, 이전 또는 완화하는 과정"으로 정의하고 있다.[8)]

우리나라 관련 기관에서 진행한 연구에서는 사이버 리스크를 "선박을 운항하는 전 과정 중에 비인가된 사용자에 의한 의도적인 장애, 손상 또는 악의적인 사용으로부터 선박 및 주변관련 대상의 컴퓨터 네트워크 및 제어시스템을 보호하는 개념"으로 정의한 바 있다.[9)]

2. 최근 사고 사례

이스라엘 사이버 보안 전문업체 Naval Dome의 북미 사업 책임자인 Robert Rizika는 "해운산업이 디지털

7 "Maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.", IMO, "Guidelines on Maritime Cyber Risk Management", MSC-FAL.1/Circ.3, 2017, Section 1.1.

8 BIMCO et al, op. cit., p.44.

9 박한선, 전게 보고서, 5면.

화됨에 따라 많은 장치와 기술 등이 온라인으로 인용돼 보안 취약점들이 발생할 것이며, 실제로 2017년 50건에 그쳤던 운영기술(OT) 시스템에 대한 사이버 공격이 2018년에는 120건, 2019년에는 310건으로 증가했고, 2020년에는 최대 900% 이상 증가할 것"이라고 전망했다.[10)]

아래에서는 최근 발생한 사이버 리스크 관련 주요 사고 사례를 살펴보고자 한다.

① 2013년 세계적인 선박연료유 공급사인 World Fuel Service(WFS)은 가짜 연료유 입찰경쟁 사기를 당해 미화 1,8000만 달러 상당의 손해를 입었다.[11)]

② 2017년 6월 세계최대의 선사인 A.P. Moeller Maersk는 그들의 전산시스템이 랜섬웨어 NotPetya의 공격을 받아 미국, 인도, 스페인, 네덜란드 소재 76개 항만에서 주문 처리와 화물운송에 지연이 발생했고 그로 인해 미화 약 3억 달러의 손해를 입었다.[12)]

③ 2018년 7월 중국 국영선사인 COSCO Shipping의 북미 롱비치항 Pier J terminal 항만운영 관련 홈페이지와 이메일 시스템이 랜섬웨어 공격을 받아 3~4일간 장애가 발생했다.[13)]

④ 2019년 2월 해커들이 미국 뉴욕과 뉴저지항으로 향하던 선박의 운항시스템을 원격 탈취하려고 시도했으나, 핵심적인 운항시스템 통제에는 실패하였다.[14)]

⑤ 2019년 3월 자동차운반선과 벌크선을 포함해 90여 척의 선박을 운용하는 우리나라 H 선사 선단 소속 일부 선박이 선내 컴퓨터가 랜섬웨어에 감염돼 선내 메인컴퓨터가 잠기는 피해가 발생했다. 감염된 선박의 컴퓨터를 모두 포맷하고 해당 컴퓨터 내의 손실된 자료를 처음부터 재작성하는 방식으로 대응해 심각한 손실은 방지했다.[15)]

10 김우정, "2018-20년, 해양산업 OT 사이버 공격 900% 증가...올 연말 최고 기록 예측", 2020. 9. 14., 해양한국, http://www.monthlymaritimekorea.com/news/articleView.html?idxno=27754.

11 Ship & Bunker world news, "WFS in court over $18M bunker scam claim", 2014.10.13., https://shipandbunker.com/news/world/670152-wfs-in-court-over-18m-bunker-scam-claim.

12 Reuters, "Cyber attack hits shipper Maersk, causes cargo delays", 2017. 6. 28., https://www.reuters.com/article/us-cyber-attack-maersk/cyber-attack-hits-shipper-maersk-causes-cargo-delays-idUSKBN19J0QB.

13 Wall Street Journal, "China's Cosco Shipping Hit by Cyberattack in U.S.", 2018.7.25., https://www.wsj.com/articles/chinas-cosco-shipping-hit-by-cyberattack-in-u-s-1532548557).

14 Wall Street Journal, "U.S. Coast Guard Warns Shipping Industry on Cybersecurity", 2019.6.11., https://www.wsj.com/articles/u-s-coast-guard-warns-shipping-industry-on-cybersecurity-11562837402.

15 김성호·김용훈, "한국 유명선사 선박 수척 랜섬웨어 피해...사이버보안 경각심 가져야", 2019. 3. 30., 파이낸셜뉴스, https://www.fnnews.com/news/201903300027281755.

⑥ 2020년 4월 악성 소프트웨어의 공격으로 글로벌 선사인 MSC의 홈페이지 운영이 약 일주일 간 중단되었다. 이로 인해 회사의 IT 서비스가 중단되었으나 화물 운영은 별도의 대리점 네트워크를 통해 정상적으로 운영함으로써 큰 피해는 방지했다.[16)]

⑦ Iran Shipping Line이 사이버 해킹으로 인해 시스템 붕괴 및 선박 추적 데이터 손실 등의 피해를 입은 바 있고, 미국 롱비치항, 이란 샤히드라자이항 및 벨기에 엔트워프항 등 다수의 항만의 IT 시스템도 사이버 공격을 받은 바 있다.

그 밖에도 선박 및 항만 등 해운물류 전반에 대한 사이버 공격은 수차례 발생했고, 현재에도 지속적으로 발생하고 있다. 해운산업이 디지털화, 네트워크화, 자동화됨에 따라 사이버 공격 시도는 점차 증가할 것이고, 사이버 공격 발생 시 피해규모도 점차 커질 것으로 예상된다.

일반적으로 사이버 공격에 따른 피해의 형태는 우선 사업 중단에 따른 영업이익 상실, 시스템 복구 등을 이유로 해커가 요구하는 보석금 및 컴퓨터 복구비용 등의 금전 손실, 기업 평판 손실 등이 있다. 해운산업에 고유한 사이버 리스크의 유형은 랜섬웨어, 화물취급시스템 오류에 따른 오배송 및 도난, 운항시스템 해킹을 통한 선박 탈취, 데이터 도난, 항만국의 제재, 선급 유지 문제 등이 있다.[17)]

영국의 한 보고서에서는 조직화된 사이버 공격으로 인해 15개 아시아지역 항만에 미치는 경제적 손실은 최소 미화 408억 달러에서 최대 1,098억 달러에 달하는 것으로 추정된다.[18)] 이러한 심각한 피해를 막기 위해서 사이버 리스크 에 대한 대응이 필수적인데, 아래에서는 이를 대비하기 위한 국제해사기구(IMO), 발틱국제해운동맹(BIMCO), 국제선급연합회(IACS) 등 해운 관련 국제기구의 해상 사이버 리스크 관련 동향을 검토하고, 이를 통해 시사점을 도출하고자 한다.

16 Lloyd's List, "MSC shutdown throws spotlight on cyber security", 2020, p.5.

17 Simon Cooper, "Cyber Risk, Liabilities and Insurance in the Marine Sector" in Baris Soyer and Andrew Tettenborn(ed)., Maritime Liabilities in a Global and Regional Context, informa law from Routledge, 2019, pp.103~105.

18 Cambridge Center for Risk Studied, "Shen attack: Cyber risk in Asia Ports", CyRim Report 2019, p.6.

Ⅲ. 국제기구의 대응

1. 국제해사기구(IMO)의 대응

(1) 해상 사이버 리스크 관리에 대한 결의안

2017년 6월 국제해사기구(IMO)는 제98차 해사안전위원회(MSC)에서 "안전관리에 관한 국제협약(International Safety Management Code, ISM Code)"[19]과 "선박 및 항만시설보안에 관한 국제협약(International Ships and Port Facility Security Code, ISPS Code)"에 "해상 사이버 리스크 관리에 관한 결의안(MSC.428(98))"을 채택하였다.[20][21]

이 결의안은 선주, 선급, 항만운영자 등 해운산업의 다양한 이해관계자들이 해상 사이버 위협의 심각성과 취약성을 스스로 인식하도록 하고, 특히 선주와 선박관리회사가 2021년 1월 1일까지 국제안전관리규약(ISM Code)의 목적과 기능 요건을 반영하여 기존 선박의 안전관리시스템(Safety Management System, SMS)내에 해상 사이버 보안 및 위험관리에 관한 내용을 포함하여 사이버 리스크에 대한 관리·운용 및 이행에 관한 사항을 적절히 반영하도록 권고하고 있다.[22]

2020년 1월 1일 이후 회사의 '이행문서'에 대한 1차 연례 검증을 실시할 예정인데, 이와 관련된 사항의 불이행이 확인되면 항만국통제(PSC) 검사 시 선박이 각 국의 항만에서 출항정지 등의 제재를 받을 수도 있다.[23]

19 ISM(International Safety Management) Code는 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 국제해상안전인명협약(SOLAS)의 제9장으로 1994년에 채택된 협약이다.

20 IMO, "Maritime Cyber Risk Management in Safety Management", Resolution MSC.428(98), adopted on 16 June 2017.

21 이현균, "자율운항선박의 운항 관련 책임에 관한 연구", 고려대학교 법학박사 학위논문, 2018, 112면.

22 "ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021" (section 2, Resolution MSC.428(98), 2017).

23 이현균·권오정, 전게 논문, 241면.

(2) 해상 사이버 리스크 관리에 관한 가이드라인

1) 개요

해사안전관리위원회에서는 2017년 해상 사이버 리스크 관리에 관한 결의안과 함께 결의안에서 언급하고 있는 해상 사이버 위험 관리에 대한 원칙적인(high-level) 권고사항을 제공하는 "해상 사이버 리스크 관리에 관한 가이드라인(MSC-FAL.1/Circ.3)"을 승인하였다.

2) 주요 내용

해상 사이버 리스크 관리에 관한 가이드라인은 해상 사이버 리스크 기능적 요소를 아래와 같이 제시하였다.

① 식별(identify): 사이버 위험관리에 대한 개인의 역할 및 책임을 정의하고 장애가 발생할 수 있는 선박운용시스템, 자산, 데이터 및 기능 등을 식별하는 것

② 보호(protect): 위험통제 프로세스, 조치 및 비상계획을 수립하여 사이버 사건에 대처하고 해상운송의 연속성 보장하는 것

③ 탐지(detect): 적시에 사이버 사건을 탐지하기 위한 프로세스와 방어수단을 개발하고 적용하는 것

④ 대응(respond): 사이버 사건으로 손상된 사업운용이나 서비스에 필요한 시스템을 복구하고 복원력을 제공하기 위한 활동이나 계획을 개발하고 구현하는 것

⑤ 복구(recover): 백업을 위한 수단을 확보하고 사이버 사건으로 손상된 해상사업을 운용하기 위한 사이버 시스템을 복원하는 것

3) 가이드라인의 성격

국제해사기구(IMO)는 스스로 가이드라인의 성격을 원칙적인(high-level) 권고사항으로 규정하고 있다.[24] 즉, 국제해사기구(IMO)의 가이드라인은 원칙적인 사항에 대해서만 언급하고 보다 구체적인 사이버 리스크 관리방안은 관련 단체 또는 각 국가의 요구사항들을 참고하도록 하고 있다. 다만, 국제해사기구(IMO)는 발틱국제해운동맹(BIMCO) 등에서 작성한 외부 자료에 대한 책임이 없음을 분명히 하고 있다.

구체적으로 가이드라인 제4조 모범사례(best practices for implementation of cyber risk management)에서는 구체적인 해상 사이버 리스크 관리방안은 회원국 혹은 기국(flag state)의 요구사항을 참고하도록 하고 있다. 또한, 해운단체인 BIMCO 등에서 작성한 '선박 사이버 보안에 관한 가이드', 국제표준기구 국제전기기술위원회의 '정보기술에 관한 기준', 미국국립표준연구소의 '중요한 기반설비의 사이버보안 개선을 위한 구조' 등을 참조하도록 권고하고 있다.[25]

24 IMO, "Guidelines on Maritime Cyber Risk Management", MSC-FAL.1/Circ.3, Secrion 2. 3. 3., 2017.

25 4.2 Additional guidance and standards may include, but are not limited to:
1. The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
2. ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems. Requirements. Published jointly by the International Organization for Standardization(ISO) and the International Electrotechnical Commission(IEC).
3. United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity(the NIST Framework).", IMO, "Guidelines on Maritime Cyber Risk Management", MSC-FAL.1/Circ.3, 2017.

2. 발틱국제해운동맹(BIMCO)의 대응

(1) 개요

세계 최대의 해운단체인 발틱국제해운동맹(BIMCO)[26]은 7개 해운단체[27]와 함께 2016년 2월에 '선박의 사이버보안에 관한 가이드라인(The Guidelines on Cyber Security Onboard Ships)' 1.1버전을 발표했다.

발틱국제해운동맹(BIMCO)은 사이버 보안 위협의 지속적인 진화에 따라 새로운 대응방안을 제시하기 위해 가이드라인을 계속 수정·보완하고 있고, 2017년 6월 2.0버전, 2018년 12월 3.0버전을 차례로 발표하였다. 또한, 현재 진행되고 있는 3.0버전에 대한 평가를 거쳐 2020년 말 새로운 버전의 가이드라인을 발표할 예정이다.

(2) 목적

이 가이드라인은 국제해사기구(IMO) "결의안 MSC.428(98)"과 국제해사기구(IMO)의 가이드라인의 내용에 맞추어 해상 사이버 보안과 사이버 안전을 포함하는 해상 사이버 리스크 관리에 관한 실질적인 권고사항을 제공하기 위해 개발되었다. 따라서 선박 소유자 및 운영자에게 회사 시스템의 사이버 보안을 유지하고, 선박에 안전하게 운항하기 위한 절차와 조치들을 규정하고 있다.

(3) 사이버 리스크 관리의 기본 원칙

① 선박의 사이버 리스크 관리 실패로 인해 발생하는 안전상·보안상·영업상 위험에 대한 인식 제고

② 선박 정보통신 및 연결 장비 보호

③ 필요한 정보에 대한 적절한 접근 보장을 위한 사용자 인증 및 허가 시스템

26 발틱해운동맹(Baltic and International Maritime Conference)은 세계 최대의 선박소유자, 용선자, 선박브로커 및 대리점의 비정부기구(NGO) 단체이다. 톤수 기준으로 세계 상선대의 약 60%가 회원으로 가입되어있고 120개국에 걸쳐 약 1,900개 선사를 회원으로 두고 있다. BIMCO, https://www.bimco.org/about-us-and-our-members.

27 InterManager, International Association of Dry Cargo Shipowners(INTERCARGO), International Association of Independent Tanker Owners(INTERTANKO), International Chamber of Shipping(ICS), International Union of Marine Insurance(IUMI), Oil Companies International Marine Forum(OCIMF), World Shipping Council 등 7개 단체.

④ 선박 환경에 사용되는 자료를 정보의 민감도에 근거해 적절히 보호

⑤ 개별적인 사용자가 인증된 정보에 대해서만 접근권한을 갖도록 적절한 IT 관리 권한 부여

⑥ 선박과 해안의 통신 관리

⑦ 위험도 평가에 근거한 사이버 사고 대응계획 수립 및 시행

4) 주요 내용

가이드라인은 다음의 내용을 포함한다.

① 선박의 안전관리시스템(Safety Management System, SMS)내에 사이버 리스크 관리에 관한 국제해사기구(IMO)의 요구를 반영하기 위한 권고사항

② 사이버 리스크 관리를 위한 구체적인 방안

- 해안 및 선박 내 사용자, 주요 인력 및 경영진의 역할 및 책임 파악
- 시스템, 자산, 데이터, 기능 등을 파악하여 교란 시 선박 운항 및 안전에 위험을 초래할 수 있음
- 사이버 사고에 대한 보호와 운영의 연속성 확보를 위한 기술적·절차적 조치의 이행
- 사이버 사고에 대한 대비 및 대응을 위한 활동 실시

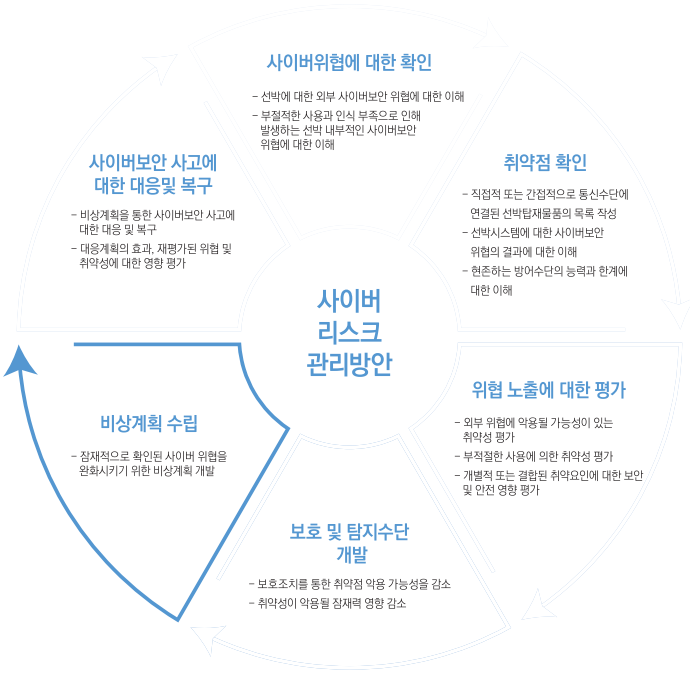
③ 운영기술(OT)의 위험 측정에 관한 추가 정보

④ 선박의 물류 공급망과 관련된 위험관리 기준 보완

⑤ 잠재적 문제를 설명하고 강조하기 위한 선박의 사이버 사고 사례

특히, 가이드라인에서 가장 중요한 것은 국제해사기구(IMO) 결의안의 요구를 수용하여 사이버 리스크 관리방안을 이행하기 위한 실질적인 권고사항이다. 가이드라인은 선박소유자 혹은 운영자에게 그들의 선박에서 사이버 사고에 대한 대응 및 복원력을 강화하기 위한 절차를 개발하고 운영하는 방법에 대한 기준을 권고하고 있다.

〈그림-3〉 BIMCO 가이드라인에 명시된 사이버 리스크 관리방안[28)]



즉, 〈그림-3〉에서 명시된 바와 같이 사이버 보안 관련 위협과 취약점을 식별하고, 위험의 크기를 측정하며, 위험을 방어하고 탐지하는 방법을 개발한다. 또한 비상계획을 수립하고 사이버 사고 발생 시 복구하고 대응하는 절차를 포함한다.[29)]

가이드라인은 〈그림-3〉의 접근방식에 따라 사이버 보안 관리 프로그램의 개발, 실행 및 유지·보수하는 것은 작은 일이 아니기 때문에 고위 경영진이 적극적으로 사이버 리스크 관리의 주도적인 역할을 수행해야 함을 강조한다. 즉, 잠재적 사이버 사고의 위협, 취약성, 위험 노출 및 결과와 관련하여 보호 및 대응 계획이 적절하게 이루어지도록 고위 경영진이 사이버 리스크 관리 전반에 걸쳐 지속적으로 관여해야 한다고 권고하고 있다.

28 BIMCO et al, op. cit., p.4.
29 BIMCO et al, op. cit., p.5.

또한 사이버 리스크 관리를 위한 일부 단계에서 기업의 상업적으로 민감한 정보나 기밀 정보가 포함될 수 있는데, 이러한 정보를 적절하게 보호하기 위해 가능한 한 민감한 정보를 자신의 안전관리시스템(SMS)에 포함하지 않도록 권고하고 있다.

3. 국제선급연합회(IACS)의 대응

(1) 개요

국제선급연합회(IACS)는 국제해사기구(IMO)의 결의안 채택 이전부터 해운산업의 여러 분야의 전문가들과 사이버 시스템에 관한 워킹 그룹을 구성하여 선박과 관련된 사이버 사고에 대한 대응방안을 모색해 왔고, 2018년 9월 선박에서의 사이버보안 관련 12가지 권고사항을 포함하는 가이드라인을 발표했다.

(2) 가이드라인의 주요 내용

가이드라인에 포함된 12가지 권고사항은 다음과 같다.

① 선박 장비 및 시스템의 소프트웨어 관리를 위한 권고 절차

② 소프트웨어 기반 기관시스템에 대한 수동/국지적 통제 역량과 관련된 권고사항

③ 선상 컴퓨터 기반 시스템의 비상계획안

④ 네트워크 설계사양(방식)

⑤ 데이터 보존

⑥ 선상 컴퓨터 기반시스템의 물리적 보안

⑦ 선상 컴퓨터 기반시스템의 네트워크 보안

⑧ 선박 시스템 설계

⑨ 컴퓨터 기반 시스템의 재고 목록

⑩ 일관적 통합

⑪ 원격 접속절차 최신화

⑫ 통신과 시스템 경계(인터페이스)

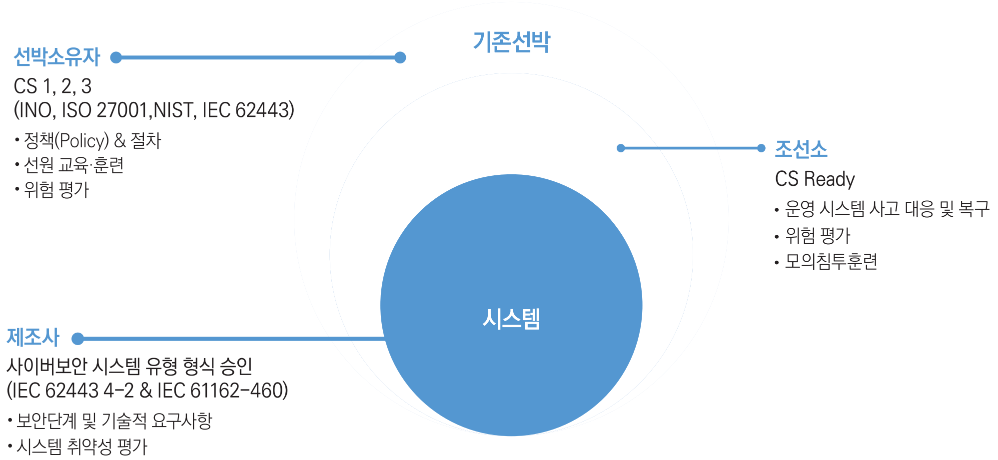
(3) 사이버 보안 형식 승인

국제선급연합회(IACS)에 속한 각 회원 선급기관은 해상사이버보안 관리시스템에 인증체계를 구축하고 선박회사 및 선박에 대한 사이버 보안 인증서비스 및 선박의 네트워크 및 자동화시스템에 대해 사이버 보안 형식승인 서비스를 제공하고 있다.

한국선급(KR)도 〈그림-4〉에서 보는 바와 같이 해상 사이버보안 인증 및 형식 승인 서비스를 제공하고 있다. 사이버보안 관리 시스템을 갖춘 선박이 인증심사(서면 및 현장검사)를 통과하면 기존선박은 적합성 인증서, 신조선은 'CS Ready 부기부호'가 부여된다. 기존선박은 사이버보안 성숙도에 따라 CS1, CS2, CS3 등 3단계로 구분되며, 36개 영역 144개 항목의 검사를 받게 된다. 신조선은 ① 선박 네트워크 구성도, 자산 목록, 시스템 기능요구사항 명세서, 사고 대응 및 복구 매뉴얼 등에 대한 문서검사, ② 선박 내 IT 및 OT 시스템에 대한 사이버 리스크 평가, ③ 사이버 보안시스템 현장검사, ④ 취약성 진단 및 침투테스트를 거쳐 CS Ready 부기부호를 부여해 건조단계부터 통합 시스템 구축·검증하고 있다.

또한 기자재에 대해서는 제조업체를 대상으로 사이버보안 기능에 대한 요구사항을 확인하여 사이버 보안 형식승인을 하고 있다.

〈그림-4〉 한국선급 사이버보안 인증 체계[30)]



Ⅵ. 시사점 및 결론

해운분야의 환경과 안전 등에 관한 총괄적인 책임을 수행하고 있는 국제해사기구(IMO), 선사 및 선박 운영사 등 운영기관을 대표하는 해운기관인 발틱국제해운동맹(BIMCO), 그리고 선박의 보험 가입 등을 위해 선박의 안전을 검사하고 평가하는 선급기관의 국제기구인 국제선급연합회를 포함한 여러 해운단체에서 해상 사이버 리스크에 대해 본격적인 논의를 시작하였다.

하지만 현재의 논의는 규제 또는 강행적인 성격의 지침 수준에는 이르지 못하고 권고사항에 그치고 있다. 비록 국제해사기구(IMO)의 결의안이 선박소유자 및 선박운영회사에게 2021년 1월 1일까지 기존 선박의 안전관리시스템에 해상 사이버 리스크 관리에 관한 사항을 포함해 이행하도록 권고하고 있지만, 사이버 리스크 관리에 관한 내용만을 포함하면 되고, 어느 수준까지 포함해야 될지는 가이드라인의 권고사항을 참고만 하면 되기 때문에 전적으로 각 선박소유자 및 운영회사에게 맡겨져 있는 것이다.

30 한국선급, KR Maritime Cyber Security Vol.28, 2020, 7면.

그리고 국제해사기구(IMO)의 결의안과 가이드라인은 클라우드 컴퓨터나 인공지능 혹은 물류 블록체인기술 등 새로운 사이버 위협 유입 경로 등에 대한 고려가 없는 등 급격하고 변화하는 사이버 리스크에 대해 완벽하게 대응하고 있지는 못한 실정이다.

결국 국제해사기구(IMO)의 결의안과 가이드라인은 해상 사이버 리스크에 대한 기본원칙과 임박한 위협에 대한 대응의 필요성을 촉구하는 의미로 받아들이고, 모범사례(best practice)로 언급한 해운단체나 선급협회 등에서 제시하는 구체적 지침을 참고하여 각자에게 맞는 사이버 리스크 대응방안을 수립하도록 위임하고 있다. 한편, 해운기업의 단체인 발틱국제해운동맹(BIMCO), 선급기관의 단체인 국제선급연합회(IACS)는 각 기업들의 이익을 위해 협력과 발전을 도모하는 단체이기 때문에 가이드라인의 성격 역시 참고사항에 불과하다.

점차 빈도가 증가하고, 피해규모도 커지고 있는 사이버 리스크를 고려하면 현재의 국제기구의 논의가 권고사항에 그치고 있기에 앞으로도 국제해사기구(IMO) 등에서도 구체적인 규제가 시행될 것으로 전망되고, 이에 맞추어 우리나라 선박안전법 등에서도 많은 변화가 있을 것으로 예상된다.

또한 사이버 리스크에 대한 대응 방안뿐만 아니라, 사법적인 관점에서 사고 발생 시 책임에 대한 문제에 대해서도 구체적인 논의가 필요할 것이다. 예컨대, 상법 제794조에서 규정하고 있는 감항능력주의의무 등에 사이버 리스크에 대한 주의의무 준수를 포함하는 이른바 사이버 감항능력주의의무에 관한 논의가 대표적인 것이다. 그 밖에도 사이버 리스크는 많은 법적 쟁점을 포함하고 있어 앞으로도 많은 연구와 입법 논의가 진행되어야 할 것이다.

참고문헌

- 김동민, “경남도, 해검Ⅱ 운항 등 ‘무인선박’ 실증 성공”, 연합뉴스, 2020. 9. 23, https://www.yna.co.kr/view/AKR20200923140900052?input=1195m.
- 김성호·김용훈, “한국 유명선사 선박 수척 랜섬웨어 피해...사이버보안 경각심 가져야”, 파이낸셜뉴스, 2019. 3. 30, https://www.fnnews.com/news/201903300027281755.
- 김우정, “2018-20년, 해양산업 OT 사이버공격 900% 증가...올 연말 최고 기록 예측”, 해양한국, 2020. 9. 14, http://www.monthlymaritimekorea.com/news/articleView.html?idxno=27754.
- 박한선, 해상 사이버 보안체계 강화방안 연구, 한국해양수산개발원, 2019.
- 윤영주, “AI 메이플라워호 출항 준비 끝...내년초 英 플리머스항 출발”, AI타임즈, 2020. 9. 17, http://www.aitimes.com/news/articleView.html?idxno=132285.
- 이현균, “자율운항선박의 운항 관련 책임에 관한 연구”, 고려대학교 법학박사 학위논문, 2018.
- 이현균·권오정, “해상사이버리스크에 관한 영국보험업계의 대응과 시사점”, 보험법연구 제14권 제2호, 한국보험법학회, 2020.
- 한국선급, KR Maritime Cyber Security Vol.28, 2020.
- 한국정보통신기술협회, ICT 표준화전략맵 ver.2020 요약보고서, 2019.
- BIMCO et al, “The Guidelines on cyber security onboard ships”, ver. 3, 2018.
- BIMCO, https://www.bimco.org/about-us-and-our-members.
- Cambridge Center for Risk Studied, “Shen attack: Cyber risk in Asia Ports”, CyRim Report 2019.
- IMO, “Guidelines on Maritime Cyber Risk Management”, MSC-FAL.1/Circ.3, 2017.
- IMO, “Maritime Cyber Risk Management in Safety Management”, Resolution MSC.428(98), adopted on 16 June 2017.
- Lloyd’s List, “MSC shutdown throws spotlight on cyber security”, 2020.
- Reuters, “Cyber attack hits shipper Maersk, causes cargo delays”, 2017.6.28., https://www.reuters.com/article/us-cyber-attack-maersk/cyber-attack-hits-shipper-maersk-causes-cargo-delays-idUSKBN19J0QB.
- Ship & Bunker world news, “WFS in court over $18M bunker scam claim”, 2014.10.13., https://

참고문헌

shipandbunker.com/news/world/670152-wfs-in-court-over-18m-bunker-scam-claim.

- Simon Cooper, "Cyber Risk, Liabilities and Insurance in the Marine Sector" in Baris Soyer and Andrew Tettenborn(ed)., Maritime Liabilities in a Global and Regional Context, informa law from Routledge, 2019.
- Wall Street Journal, "China's Cosco Shipping Hit by Cyberattack in U.S.", 2018.7.25., https://www.wsj.com/articles/chinas-cosco-shipping-hit-by-cyberattack-in-u-s-1532548557.
- Wall Street Journal, "U.S. Coast Guard Warns Shipping Industry on Cybersecurity", 2019.6.11., https://www.wsj.com/articles/u-s-coast-guard-warns-shipping-industry-on-cybersecurity-11562837402.

KOREA
LEGISLATION
RESEARCH INSTITUTE

최신외국법제정보

Issue Brief on Foreign Laws

KLRI

맞춤형 법제정보 신청 안내

한국법제연구원 글로벌법제전략팀은 정부부처, 공공기관 등을 대상으로 외국 법제 조사 신청을 받아, 조사결과를 무료로 제공하고 있습니다.

제공내용 정보

- 주요 국가(미국, 영국, 캐나다, 호주, 독일, 프랑스, 일본, 중국 등) 법령의 제·개정 내용
- 국내 현안에 대한 외국 법제 현황 및 내용
- 정부 입법 정책 수립에 필요한 외국 법령 정보
- 정부 부처 관련 업무에 대한 법령 정보

※ 개인적인 연구(예, 학위논문 작성) 관련 및 단순 법령은 제외되며, 내용이 지나치게 광범위하거나 모호한 범위의 정보제공은 불가능할 수 있습니다.

신청방법

- 한국법제연구원 홈페이지(www.klri.re.kr)를 통하여 신청을 받습니다.

  * 홈페이지 접속 → 좌측 하단의 수요자 맞춤 서비스 중 "맞춤형 외국법제정보 신청하기 GO" Click (회원가입 후 로그인)

- 최신외국법제정보 담당자에게 메일로 신청하실 수 있습니다.

  * 신청메일주소 : foreignlaw@klri.re.kr

  ※ 신청시, 대상 국가 법령 및 제도의 명칭 등을 구체적으로 명시하셔야 합니다.

접수 및 문의

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

TEL. (044) 861-0482
FAX. (044) 868-9919
E-Mail. foreignlaw@klri.re.kr
www.klri.re.kr

배포

- 정기간행물 형식으로 발간되고 있으며, 정부부처, 공공기관 등에 배포 중입니다.
- 신청하시는 경우 '최신외국법제정보'를 무료로 보내드립니다.

ISSN 1976-0760

미래혁신과 국민행복을
추구하는 글로벌 입법
연 구 플 랫 폼

한국법제연구원

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

발행일 2020년 11월 30일 | 발행인 김계홍 | 발행처 한국법제연구원 (www.klri.re.kr)
주소 30147 세종특별자치시 국책연구원로15 한국법제연구원
TEL (044) 861-0300 | FAX (044) 868-9913