석사학위논문

조선·해운산업 보안관리체계 분석 및 사이버보안 모델 구현 방안 연구

-선박·항만 보안체계 중심으로-

2022년

한성대학교 지식서비스&컨설팅대학원

스 마 트 융 합 컨 설 팅 학 과

스마트융합보안컨설팅전공

최 웅 재

석 사 학 위 논 문
지도교수 원종혁

조선·해운산업 보안관리체계 분석 및 사이버보안 모델 구현 방안 연구

-선박·항만 보안체계 중심으로-

Analysis of shipbuilding and shipping industry security management system and research on cybersecurity model implementation plan

2021년 12월 일

한성대학교 지식서비스&컨설팅대학원

스 마 트 융 합 컨 설 팅 학 과

스마트융합보안컨설팅전공

최 웅 재

석 사 학 위 논 문
지도교수 원종혁

조선·해운산업 보안관리체계 분석 및 사이버보안 모델 구현 방안 연구

-선박·항만 보안체계 중심으로-

Analysis of shipbuilding and shipping industry security management system and research on cybersecurity model implementation plan

위 논문을 컨설팅학 석사학위 논문으로 제출함

2021년 12월 일

한성대학교 지식서비스&컨설팅대학원

스 마 트 융 합 컨 설 팅 학 과

스마트융합보안컨설팅전공

최 웅 재

최웅재의 컨설팅학 석사학위 논문을 인준함

2021년 12월 일

심사위원장 홍 정 완 (인)

심 사 위 원 원 종 혁 (인)

심 사 위 원 박 인 채 (인)

국 문 초 록

조선·해운산업 보안관리체계 분석 및 사이버보안 모델 구현 방안 연구

한성대학교 지식서비스&컨설팅대학원
스 마 트 융 합 컨 설 팅 학 과
스 마 트 융 합 보 안 컨 설 팅 전 공
최 응 재

우리나라는 4차산업 혁명 이후의 미래융합사회를 맞이하고 있으며 스마트 융합산업의 급속한 변화에 대응해야하는 시기에 있다. 글로벌 최고 수준을 유지하고 있는 조선·해운산업에서는 ICT와 OT가 융합되어 디지털화 및 자동화가 전반적으로 전환되고 있다. 최근에는 자율운항선박과 스마트 쉽, 스마트항만에 대한 수요가 확대됨으로 인해 선박 및 항만에 대한 사이버 위협이 증가하게 되었고 이로 인해 정보보호관리체계 개선의 필요성이 증가하게 되었다. 2020년 12월에『정보통신망 이용촉진 및 정보보호 등에 관한 법률』개정되면서 융합ICT 분야도 정보보호 규율대상이 되었고 정보통신망연결기기에 선박이 교통 분야에 추가 되었으며 이에 따라 조선·해운분야에서도 정보보호의 필요성이 더욱 강조되고 있다.

선박과 부속 기자재의 자동화 및 디지털화로 인해 인터넷과 연결 접점이 증가하게 되면서 사이버보안 위협이 증가하게 되었다. 편리함을 위한 인터넷 연결은 해킹 및 악성코드 감염 등으로 인해 선박 운항이 중단되기 까지 하는

피해가 발생하였으며 이로 인해 재산상의 큰 피해가 발생하게 되었다. 2017년 6월 덴마크의 세계 최대 해운사인 A.P. Moller – Maersk가 랜섬웨어 공격을 받게 되면서 약 3천억 원 이상이라는 천문학적인 금전적 피해가 발행되었다. 그 외에도 국·내외 조선사 및 해운사, 선박 및 항만 에서도 사이버보안 침해사고가 끊이지 않고 발생하고 있다.

이에 따라 국제해사기구에서는 해상 사이버 위협으로 인해 중요한 정보나 시스템이 손상되거나 손실되어 물질적 피해를 입거나, 운송 및 운영에 있어서 시스템이 중단되는 재산상의 피해도 발생하게 되었다. 이와 같은 사이버 위협으로 인한 불안감이 급증하다 보니 최근인 2021년 1월에는 'Cyber Risk Management'를 공표하고 준수할 것을 강조하게 되었다.

본 연구 결과를 통해 조선·해운산업분야에서 발생할 수 있는 사이버보안의 문제점을 인식하고 이를 개선하기 위한 계기가 되기를 기대한다. 본 연구를 위해 국제해사기구와 국·내외 선급에서 기준하고 있는 사이버보안 지침 및 가이드라인을 분석 하였으며 발견된 문제점을 해결하기 위해 사이버보안 모듈을 구현하여 실증을 하였으며 최종적으로 개선된 관리체계를 제언하고자 한다.

향후 조선·해운산업에서의 사이버보안 수준 향상과 보안위협을 예방하는데 기여할 것으로 기대한다. 또한 우리나라 조선·해운산업이 글로벌 경쟁력 수준이 최고 수준을 유지하고 있는 만큼 향후 추가적인 연구 활동을 함으로서 국제기구 및 글로벌 선급의 기준을 충족하는 보안관리체계를 수립할 수 있을 것이다. 따라서 우리나라가 선도적 보안관리체계 모델을 제시함으로서 글로벌 해상 사이버안전지대의 파수꾼 역할을 수행할 수 있는 계기를 마련 할 수 있을 것이다.

【주요어】 선박 사이버보안 모델, 사이버 위험 관리, 해양 사이버 침해사고, 해양 사이버보안, 사이버보안 인식

목 차

표 목 차

그 림 목 차

제 1 장 서론

제 1 절 연구의 배경 및 목적

1) 연구의 배경

4차산업 혁명과 융합산업의 급속한 변화에 따라 해양산업에서 조선업과 해운업에서도 정보통신기술(ICT)[1]와 운영기술(OT)[2]가 융합되어 선박과 항만 등이 디지털화 및 자동화가 급속도로 확산되고 있다. 최근에는 자율운항선박과 스마트 쉽, 스마트항만이 확대되면서 선박 및 항만에 대한 사이버 위협으로부터 정보보호의 필요성이 증가하게 되었다. 사이버보안 강화는 금융 분야나 의료 분야, 교육 분야 등 뿐만 아니라 항만과 해운사, 선박에서도 중요하다. 보안전문가들도 해양에서 선박이 사이버보안 피해에 대한 지원이 어려움이 따른다. 선박 사이버보안 강화를 위해 선박 사이버보안 책임자와 전문 인력을 지정하고 정보보안 교육 및 훈련의 필요성은 다양한 지침서들과 선행연구를 통해 언급되고 있다.

우리나라에서는 2020년 12월에『정보통신망 이용촉진 및 정보보호 등에 관한 법률』개정되면서 융합ICT 분야도 정보보호 규율대상이 되었다. 정보통신망법 제 45조(정보통신망의 안정성 확보 등)1의 2항에 정보보호가 의무화되는 정보통신망연결기기에 선박이 교통 분야에 추가 되었으며 이에 따라 조선·해운분야에서도 정보보호의 필요성이 증가되었다.

한편 국제해사기구(IMO)[3]에서는 해상 사이버 위험이 정보나 시스템이 손상 또는 손실되어 운송 관련 운영에 안전 또는 보안 실패를 초래할 수 있는 잠재적 상황이나 사건으로 정의하고 있으며 중요성을 강조하고 있다. IMO는 2017년 6월 MSC.428(98)[4]에 'Cyber Risk Management'를 채택하고(Marin

1) ICT :Information and Communications Technology

2) OT : Operational Technology

3) IMO : International Maritime Organization, 선박의 항로, 교통규칙, 항만시설 등을 국제적으로 통일하기 위하여 설치된 UN 전문기구, https://www.imo.org

Link. 2021.11) 2021년 1월부터 'Cyber Risk Management'를 준수하는 것을 권장하고 있다.

BIMCO에서 2020년 2월부터 4월까지 설문조사한 보고서에 따르면 응답자의 31%가 1년 내에 사이버 침해 사고를 경험한 것으로 조사되었다. 가장 많이 발생한 사이버 침해 유형은 피싱 및 스피어 피싱, 멀웨어로 응답한 것으로 보아 주로 선박분야와 관련된 조직 및 구성원들이 보안 위협에 노출되었음을 시사한다.

조선·해운산업에서의 사이버보안 위협이 증가하고 있는 추세로 2017년 6월 덴마크의 세계 최대 해운사인 A.P. Moller – Maersk는 랜섬웨어 공격으로 인해 직접적인 매출 감소, 추가 근로, 수습 비용 등이 발생하게 되었으며 약 3억 달러에 달하는 금전적 피해를 입게 되었다. 이는 해사 관련 분야에서의 사이버보안에 대한 중요성과 필요성을 다시 한 번 인식하는 중요한 계기가 되었다. Maersk뿐 아니라 이란 해운과 리마솔 지역 해운기업, 미국 해안경비대, 미국 롱비치 항, 해운사 MSC 및 CMA CGM, COSCO 등에서 사이버보안 침해 사고가 지속적으로 발생하였다.

2) 연구의 목적

해사 사이버보안을 강화하기 위해서는 국내외에서 발생한 사이버보안 침해 사고 사례에 대한 실태 분석을 통해 원인을 파악해야 하고 해사 사이버보안 관련 법률과 규제, 지침, 가이드라인들의 비교분석을 통한 체계 개선이 우선적으로 필요하다.

본 논문은 조선·해운산업분야에 일어난 사이버보안 침해사고를 살펴보고 사례들의 원인을 분석하여 조선·해운산업분야에서 사이버보안의 필요성을 분석하였다. 그리고 조선·해운산업과 관련된 사이버보안 규정·지침·가이드라인을 비교 분석하여 해양 사이버보안 지침이 요구하는 것을 실무적으로 이해하고 사이버보안 관리체계 강화에 대한 개선방안을 도출하고자 한다.

4) IMO 해양안전위원회의 2017년 6월 98차 회의 결의안

제 2 절 연구의 방법

본 연구에서는 국내 및 국외의 해사 사이버보안 규제 및 지침, 가이드라인과 사이버보안 침해 사고 사례들을 비교 분석하고 해사 사이버보안 가이드의 개선대책과 강화방안에 관한 연구를 진행하였다.

제1장에서는 해사 사이버보안에 관한 연구 배경 및 연구 목적을 정의 하였다.

제2장에서는 조선산업과 해운산업에 대해 알아보고 해사 사이버보안 규정과 침해사고 사례를 알아보았으며 본 논문에서 연구하고자 하는 해사 사이버보안 강화에 대한 개념을 정리하였다.

제3장에서는 조선·해운산업 사이버보안 지침에 대한 분석과 사이버보안 침해사고 사례 분석을 통해 문제점을 인식하고 개선방안에 대해 연구하였다.

제4장에서는 조선·해운산업 사이버보안 관리체계 개선방안의 설계와 아키텍처를 개발하고 관리체계 개선대책을 구현하였다.

제5장에서는 본 논문의 결론 및 시사점과 연구의 한계점 및 향후 과제를 제시하였다.

제 2 장 이론적 배경과 선행연구

제 1 절 조선·해운산업분야 정의

1) 조선산업분야 개요

조선 산업은 사람 또는 화물을 적재하고 강이나 바다에서 항행하는 선박 또는 해양 자원을 탐사·시추·생산을 목적으로 하는 선박 및 플랜트를 건조 또는 수리하는 산업으로써 타 제조업과는 확연히 다른 특징이 있으며 크게 여섯 가지로 구별해 볼 수 있다(양해성 外, 2021). 그리고 선박법 기준에 의하면 선박은 수상 또는 수중에서 항행용으로 사용하거나 사용할 수 있는 배 종류를 지칭한다.

첫 번째, 자동차 산업의 구조와 유사하게 다양한 후방산업에 대한 파급효과가 큰 산업이다. 선형 및 선종에 따라 다소 차이가 있지만 일반적으로 선박 한 척을 건조하는데 약 460~500여 종의 기계·부품 및 자재류가 필요하며, 이는 선박 건조 비용 원가의 55~65%에 해당한다(김진근, 2008; 한국조선해양기자재연구원, 2016).

두 번째, 조선 기업은 시스템 통합 역량(System Integration Capability)을 갖추어야 한다(Sosa et al., 2004, Kiamehr et al, 2014). 시스템 통합 역량은 선박 건조에 필요한 다양한 기자재 및 소재 관련된 기술적 지식을 활용하여 설계, 기자재 조달, 건조, 테스트 등의 활동을 총체적으로 수행할 수 있는 역량을 의미한다. 이러한 시스템 통합 역량에는 의도한 선박의 기능 구현 뿐 아니라 건조 프로젝트 관리, 핵심(Core)・보완(Enabling) 기술의 선택을 포함하며 사이버보안 위협에 대비한 시스템의 적절한 설계가 필요하다(Ruuska et al., 2013; Kiamehr et al., 2014; DSLAB컴퍼니, 2021).

세 번째, 노동 집약적인 특징을 가지고 있다. 선박을 건조함에 있어 다양한 기자재를 조립해야 하거나 소재를 활용해야 하지만 프로젝트 형태의 건조로 인한 자동화에도 한계가 있기 때문에 기능 인력이 적정 규모로 확보가 되

어야 한다(이경묵 外, 2013). 이러한 특징은 조선 산업이 고용 창출 효과가 크다는 것을 의미할 뿐 아니라 전체 건조 비용에서 인건비의 비중이 산업의 경쟁력에 중요한 영향을 미칠 수 있음을 의미한다(Jiang et al., 2011; 양종서 外, 2019).

네 번째, 자본 투자가 대규모로 요구되는 특징이 있다. 선박 한척의 건조 기간이 1년 반에서 2년 정도이며 대형 유조선의 경우에는 3년 이상의 기간이 소요될 정도로 매우 긴 기간이 필요하다. 그리고 선주들이 건조 대금을 인도 시 'Heavy-Tail' 방식을 선호하여 지급하기 때문에 장기간 동안 운영할 수 있는 자금의 확보방안이 반드시 필요하다. 이에 따라 선박금융 역량 및 정책 지원이 필요하다(이경래, 2018; 곽기호, 2019). 그리고 사업시작 초기에 도크 및 크레인, 선대, 안벽 등의 다양한 인프라 투자가 필요하기 때문에 이를 감내할 수 있는 기업만이 진입이 가능하다(홍성인, 2010; 이경묵, 박승엽, 2013). 또한 진입 이후에 구형 설비의 감가상각과 신규 설비 투자 필요에 대응하고 지속가능한 경쟁력 유지를 위한 이유로 진입장벽이 높은 산업이다(Vishnevskiy et al., 2017; 양종서, 임종수, 2019; 이은창 外, 2019).

다섯 번째, 선박의 건조 및 운항과 관련하여 다양한 규제가 적용된다. 일반적으로 상선은 자유롭게 세계 어느 곳이든 다닐 수 있기 때문에 규제의 초국가적(Transnational)인 지리적 적용 범위(장세진, 2019)가 매우 제한적이라는 특징이 있다. 그 범위는 내용적 범위, 해양오염, 승무원 근무 위생·환경, 화물 안전, 보안 등 매우 다양하다(이경묵, 박승엽, 2013). 특히 최근 들어 국제해사기구(IMO)를 중심으로 SOx(황산화물), NOx(질소산화물) 및 CO2와 같은 배기·온실가스 규제가 전 세계적으로 강화되고 있어 이에 대한 대응이 기업 경쟁력에 큰 영향을 미치고 있다(이언경, 2011; 법제처, 2019; 하나금융투자, 2020). 그리고 각국 정부는 선주들을 규제하여 선박 건조에 필요한 기자재 및 인력, 서비스, 인프라의 일정 비중 이상을 자국에서 생산하게 하거나, 자국 생산품을 활용할 것을 의무화하는 등의 현지조달법(Local Contents Act) 적용을 강화하고 있다.

마지막으로 세계 에너지 시장 수요·공급 및 정책에 민감한 영향을 받는다. 2016년 기준 세계 해상물동량의 구성 화물은 에너지원 중에서 약 38.0%

의 비중으로 원유, 석유제품 및 가스 등을 가장 높은 비중을 차지하고 있고 이는 세계 에너지 시장에 직간접적으로 영향을 받는 것을 의미한다(홍성인, 2017). 지난 2011년 일본 후쿠시마 원전사고로 천연가스 수요가 급증하면서 단기간에 LNG Carrier 시장이 급성장하였다(이은창 外, 2019; 양종서, 임종수, 2019). 그리고 2013년 이후 미국의 셰일가스 수출과 호주 천연가스 생산설비 증설은 LNG 가격을 하락시키면서 선박의 연료로 LNG를 사용하고자 하는 수요도 최근 크게 늘어나고 있다(하나금융투자, 2020).

2) 해운산업분야 개요

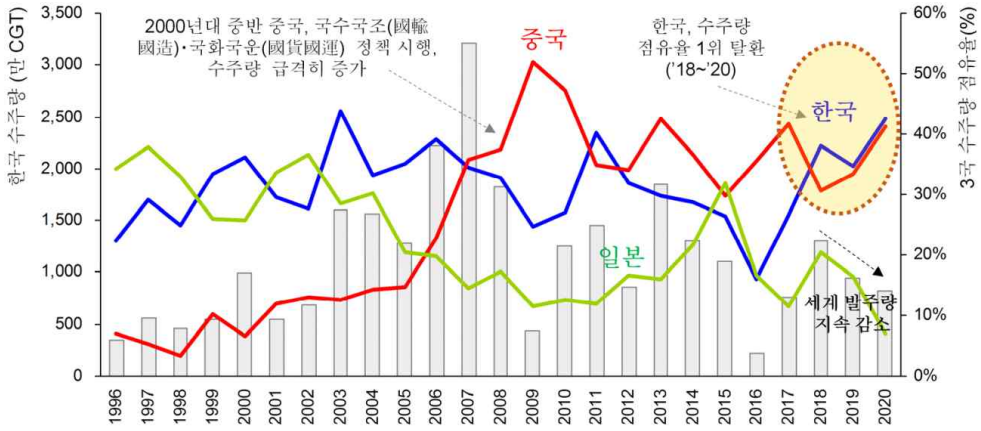
항만은 선박의 출입, 사람의 승선·하선, 화물의 하역·보관 및 처리, 해양친수활동 등을 위한 시설과 화물의 조립·가공·포장·제조 등 부가가치 창출을 위한 시설이 갖추어진 곳을 의미한다(항만법, 2020).

이석호(2009)의 연구에서는 해상운송(Sea Transport, Shipping, Ocean Shipping)은 바다를 통로로 운송수단인 선박을 이용하여 화물이나 여객을 이전하는 경제적 활동(Economic Activities)인 교통산업의 하나로 정의하고 있다. 해상운송은 인적요소, 물적 요소, 해운수요 세 가지 기본 요소로 구성되어 있다. 인적요소는 선박 운항을 하는 선장 및 선원, 물적 요소는 운송 수단이 되는 선박, 해운수요 객체는 화물 및 여객을 의미한다. 따라서 해운은 사람과 재화 상호간에 물리적, 공간적 간격을 극복하기 위한 사회적·경제적 이동활동을 할 수 있는 교통의 일부이다. 교통은 운송과 통신으로 넓은 의미에서 구분되며 운송은 다시 도로운송과 철도운송과 같은 육상운송, 해상운송과 내수운송과 같은 수상운송, 그리고 항공운송으로 구분할 수 있다고 말한다.

최근에는 해운·물류산업에도 4차 산업혁명에 의한 융합적 이슈가 증가하게 되었다. EU와 일본의 해운·물류산업은 IoT, AI 등의 기술을 활용한 자동운항선박이나 원격조정선박 개발 등을 추진 중에 있으며 이를 통해 안전 운항 제고와 운항 효율 향상 등을 도모하고 있다.(박영태 外, 2020; 안영균 外, 2021)

3) 조선·해운산업분야 시장

조선 산업의 주도권은 아래 [그림 2-1]과 같이 2018년을 기점으로 수주량 기준으로 보았을 때 중국에서 우리나라로 주도권이 이전되었음을 알 수 있다. 우리나라는 2018년에 1,341만 CGT[5] 수주하여 38.1%의 수주 점유율을 기록하면서 30.6%의 중국을 넘어섰다. 그리고 2020년에는 코로나 팬데믹에 따른 발주량 감소에도 불구하고(김성현, 2020; 조선비즈, 2020) 2020년 하반기 집중수주를 통해 3년 연속으로 42.6%의 수주 점유율 1위를 기록하였다. 이러한 성과는 2018년부터 2020년 사이 수주 실적 중에서 중국은 자국 선사 발주 비중이 69.2%이고 일본은 자국 선사 발주 비중이 42.8%, 우리나라는 자국 선사 발주 비중이 17.2%로 중국과 일본과 비교하였을 때 2.5~4배에 달한다는 점에서 더욱 의미 있는 성과로 평가하고 있다(양해성 外, 2021).

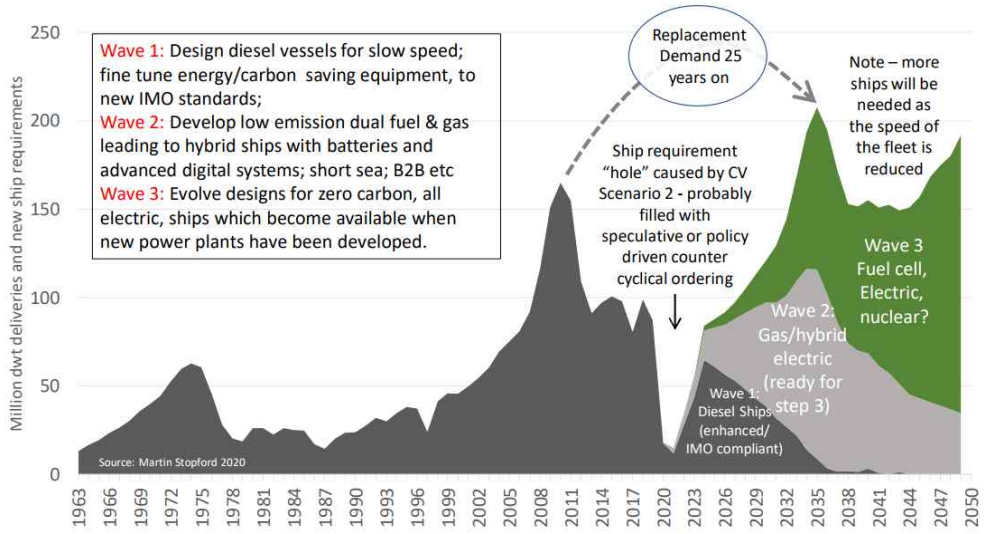


[그림 2-1] 수주량 기준 우리나라와 중국의 세계 조선시장 점유율 추이(양해성 外, 2021)

Martin Stopford(2020)는 오늘날 전 세계 5000톤 이상 화물 운송선(GT)의 99% 이상이 화석 연료에 의존하고 있으며 이 중 78%는 2행정 디젤 엔진, 17%는 4행정 디젤, 4%는 디젤 전기, 1%는 증기 터빈으로 이 규모에 비

5) CGT : Compensated Gross Tonnage, 표준선환산톤수

해 비화석 연료 추진 선박은 7척의 쇄빙선 뿐이라는 조사결과를 언급하였다. IMO 규제는 2050년까지 배출량이 2008년의 절반 미만이어야 한다고 규정하고 있다. 배출량이 정확하게 계량되지는 않지만 2008년 수준은 약 9억 톤의 탄소에서 2050년 약 4억 5천만 톤으로 감소함을 의미한다고 하였다. 가스 및 하이브리드 추진 선박은 기술적 정교함에도 불구하고 대량 및 라이너 무역에서 성공할 수 있을 만큼 저렴하고 신뢰할 수 있으며 상업적으로 강력한 설계를 개발하는 데 중요한 시험장이 될 것이다. 토지 수요가 많은 따라서 탄소 문제를 충족하려면 단계적 접근 방식이 수반되어야 하며 아래 [그림 2-2]는 표시된 세 가지 기술 웨이브 2020-2050에서 설계 혁신이 도입될 것을 설명하고 있다. 제1의 물결은 디젤선박의 생산이 불가피하게 수반되어야 한다. 디젤 엔진은 매우 효율적이며 제로 카본 대안이 없기 때문에 가장 효과적인 옵션은 디젤 엔진에 대한 투자를 지속하는 동시에 전체 선상 플랫폼의 성능을 향상시키는 것이다. 제2의 물결은 가스 및 하이브리드 동력 선박을 포함하는데 이 선박은 2020년대 초에 시작되어 이 기간이 끝날 때까지 계속된다. 가격 책정은 이 파동이 어떻게 전개되는지를 결정하는 데 중요한 역할을 할 것이다. 배터리를 사용하는 가스와 하이브리드 선박은 기술적 정교함에도 불구하고 대량 및 라이너 무역에서 성공할 수 있을 만큼 저렴하고 신뢰성이 높으며 상업적으로 강력한 설계 개발을 위한 중요한 시험장을 나타낸다. 처음에는 기존 선박보다 더 비쌀 가능성이 높으며 탄소 배출량이 약 20~30% 감소하기 때문에 이를 보완하기 위해 충분히 높은 시간 용선료를 유치해야 한다. 그리고 제3의 물결은 탄소 제로 추진 시스템으로 현재 계획에서 벗어나 확장성 문제에 직면해 있다. 1세대 상용 연료 전지 및 배터리 추진은 2020년대 중반에 가능할 수 있다. 벙커 네트워크를 개발하는 것 또한 이러한 위험한 상품을 유통하는 데 있어 기술적, 안전상의 문제로 인해 시간이 걸릴 것이다. 마지막으로 추진 시스템과 벙커는 탄화수소보다 훨씬 더 비쌀 수 있다. 그래서 투자자들은 그들이 무엇을 하든 어려운 결정에 직면할 것이다(Martin Stopford, 2020).



[그림 2-2] Technology scenario 2 to reach IMO 2050 CO2 target(Martin Stopford, 2020)

이재성과 박세훈(2021)의 연구에 따르면 우리나라의 전체 운항 가능 선복량도 한진해운 파산을 기점으로 이전 105만 TEU 수준에서 39만 TEU로 62% 감소하였으며 글로벌 해운시장에서 우리나라 선사들이 차지하는 시장 점유율 또한 5% 이상에서 1.6%로 3분의 1 수준으로 감소하였다(이재성, 박세훈, 2021). COVID-19 팬데믹 상황 하에서 수출은 2020년 1월에서 5월까지 전년 동기와 비교하여 11.4% 감소하였으나 동 년 6월부터는 회복하기 시작하여 감소폭을 점차 줄여나갔다. 이후 2021년 1 월에서 3월까지의 수출액은 전년 동기 대비 9.5% 증가하였다. 2021년 1월~2월에는 우리나라의 주요 수출시장 가운데 EU 35.5% 증가, 미국 26.6% 증가, 중국 24.5% 증가한 반면 ASEAN의 경우 11.5% 감소하였다. 전체적으로 수출이 급속한 회복세를 보이는 가운데 COVID-19 영향 이전의 상황과 비슷한 수준에 이르렀다.(이재성 外, 2021; 조성대, 2021)

제 2 절 사이버보안 규정

1) 정보보안 법제도

‘정보보호’의 법적 개념은 『정보보호산업의 진흥에 관한 법률』 제2조의 제1항 제1호 가목에 “정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것”과 나목에 “암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것”의 “활동을 관리적·기술적·물리적 수단을 마련하는 것”으로 정의되어 있다.

우리나라의 정보보안 관련 법제도는「국가사이버안전관리규정」과 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』,『정보통신기반 보호법』,『개인정보보호법』,『신용정보의 이용 및 보호에 관한 법률』 등이 있다. 해외 주요국의 정보보안 관련 법제도로 미국은 1980년대에는 『컴퓨터 보안법(Computer Security Act of 1987)』과 2000년대에 들어서 제정된 『국토안보법』이 있고(홍순좌, 2019) 일본의 『디지털청 설치법』과 『디지털 사회의 형성을 도모하기 위한 관계 법률의 정비에 관한 법률』, 『공적 급부의 지급 등의 신속하고 확실한 실시를 위한 예저금 계좌의 등록 등에 관한 법률』,『예저금자의 의사에 근거한 개인번호 이용에 의한 예저금계좌의 관리 등에 관한 법률』,『지방공공단체 정보 시스템의 표준화에 관한 법률안』이 있다(김경석. 2021).

현재 우리나라의 사이버보안과 관련한 법령을 살펴보면 일반적인 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호하기 위한 목적으로 제정된 「국가사이버안전관리규정」만 있었고(이은수 外, 2021), 최근 2020년 12월에『정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭:정보통신망법)』이 개정되면서 제 45조(정보통신망의 안정성 확보 등)1의 2항에 정보통신망연결기기의 범위가 가전, 교통, 금융, 스마트도시, 의료, 제조·생산, 주택, 통신 등으로 확대되었고 교통 분야에 선박이 추가되었다.

우리나라의 정보보호 추진체계는 부문 별로 공공부문과 민간부문, 주요정

보통신기반시설로 구분하여 적용할 수 있다. 공공부문은 「국가사이버안전관리규정(대통령훈령 제316호)」에 의하여 구성되고 민간부문은 정보통신망 이용촉진 및 정보보호 등에 관한 법률』에 의해 구성된다. 그리고 주요정보통신기반시설은 『정보통신기반 보호법』에 의하여 구성된다.

먼저 공공부문에 대한 정보보호 추진체계는 법제처 국가법령정보센터에 「국가사이버안전관리규정(대통령훈령 제316호)」가 2005년에 제정되어 2013년까지 5차례에 걸쳐 개정되었고 이에 의하여 구성되어 있다. 당해 규정(훈령)은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다(제1조). 당해 규정에 따라서, 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 총괄 조정한다(제5조제1항). 그리고 국가정보원장 소속 하에 국가사이버안전전략회의, 국가사이버안전대책회의, 국가사이버안전센터를 둔다(제6조 내지 제8조). 한편 중앙행정기관의 장은 소관 정보통신망을 보호하기 위하여 사이버안전대책을 수립·시행하고, 이를 지도·감독하여야 하고(제9조제1항), 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지 분석하여 즉시 대응 조치를 할 수 있는 보안관제센터를 설치 운영하여야 하며(제10조의2제1항), 사이버안전에 위협을 초래할 수 있는 정보 등을 입수한 경우에는 국가안보실장 및 국가정보원장에 통보하여야 한다(제10조제1항). 이 경우 국가정보원장은 제공받은 정보 관련 대응 조치를 강구한 후 그 결과를 해당 기관에 통지한다(제10조제2항). 국가정보원장은 사이버공격을 탐지한 경우 사이버공격경보를 발령하며, 심각 수준의 경보는 국가안보실장과 협의하여 발령한다(제11조).

한편 사이버공격으로 인한 사고 발생 또는 징후를 발견한 경우 중앙행정기관의 장은 피해를 최소화하는 조치를 취하고, 지체 없이 그 사실을 국가안보실장 및 국가정보원장에게 통보하여야 한다. 마찬가지로 지방자치단체의 장 및 공공기관의 장은 피해를 최소화하는 조치를 취하고, 그 사실을 지체 없이 국가안보실장, 국가정보원장 및 관계 중앙행정기관의 장에게 통보하여야 한다(제12조). 국가정보원장은 사고의 원인을 분석하기 위한 조사를 실시할 수 있

으며, 피해가 심각한 경우 사이버위기 대책본부를 구성할 수 있다. 또한 국가정보원장은 사이버공격에 의한 피해 및 대책본부의 대응상황을 국가안보실에 통보하고, 국가안보실장은 이를 종합하여 대통령에게 보고한다(제13조). 그리고 국가정보원장은 사이버 안전관련 연구개발에 필요한 시책을 추진하며, 중앙행정기관의 장은 국가보안기술연구소로 하여금 연구개발을 수행하게 할 수 있다(제15조).

다음으로 민간부문의 정보보호 추진체계는 법제처 국가법령정보센터에 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』에 의해 구성되어 있다. 정보통신망법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다(제1조).

정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 정보보호 최고책임자를 지정할 수 있으며, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다(제45조의3제1항). 그리고 정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다(제45조제1항). 또한, 타인의 정보통신 서비스 제공을 위하여 집적된 정보통신시설을 운영 관리하는 집적정보통신시설 사업자는 정보통신시설을 안정적으로 운영하기 위한 보호조치를 하여야 한다(제46조).

한편 과학기술정보통신부장관은 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치의 구체적 내용을 정한 정보보호지침을 고시하고(제45조제2항), 정보통신서비스 또는 전기통신사업을 시행하고자 하는 자에게 정보보호 사전점검기준에 따른 보호조치를 권고할 수 있으며(제45조의2제2항), 정보보호 관리등급 부여(제47조의5) 및 정보보호 관리체계를 운영하는 자에 대한 인증을 할 수 있다(제47조). 그리고 주요정보통신서비스 제공자 및 집적정보통신시설 사업자는 침해사고 관련 정

보를 과학기술정보통신부장관이나 한국인터넷진흥원에 제공하여야 한다(제48조의2제2항). 이에 대해서 과학기술정보통신부장관은 침해사고 관련 정보의 수집 전파, 침해사고의 예보 경보, 침해사고에 대한 긴급조치를 수행하고, 필요한 경우 이를 한국인터넷진흥원이 수행하도록 할 수 있다(제48조의2제1항).

주요정보통신기반시설에 대한 정보보호 추진체계는 법제처 국가법령정보센터에 『정보통신기반 보호법』에 의하여 구성된다. 정보통신기반 보호법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립 시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다(제1조). 여기서 '정보통신기반시설'이라 함은 국가안전보장 행정 국방 치안 금융 통신 운송 에너지 등의 업무와 관련된 전자적 제어 관리시스템 및 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 가공 저장 검색 송신 또는 수신하는 정보통신체제인 정보통신망을 말한다(제2조 제1호).

하지만 선박과 항만에 대한 직접적인 정보보안 법제도는 아직 제정되지 않았으며 『선박안전법』과 『해사안전법』, 『국제항해선박 및 항만시설의 보안에 관한 법률』에서 정보보안에 대한 개정이 필요성을 느끼고 선박 사이버보안 관련 법률의 제정이 필요한 시점이다(이은수, 2021).

2) 사이버보안 지침

우리나라의 사이버보안에 대한 지침 및 가이드라인으로 '정보보호 및 개인정보 관리체계'와 기반시설을 대상으로 하는 '주요정보통신기반시설 기술적 취약점 분석평가 방법 상세가이드', 금융 분야의 '금융권 정보보호 및 개인정보보호 관리체계' 및 '전자금융기반시설 보안 취약점 평가기준', 의료기기에 적용되는 '의료기기 사이버보안 가이드라인' 등이 있다.

'정보보호 및 개인정보 관리체계'는 정보보호 관리체계(ISMS[6])와 개인정보보호 관리체계(PIMS[7]) 두 개의 인증제도의 인증에 대한 부담감의 문제를

6) ISMS : Information Security Management System

7) PIMS : Personal Information Management System

해소하고자 업계의 의견들을 고려하여 인증 제도를 통합 개편하였다. 과학기술정보통신부, 행정안전부, 방송통신위원회는 ISMS와 PIMS 인증을 통합한 ISMS-P[8] 고시안을 마련하여 행정예고를 통해 국민 의견수렴 과정을 거쳤다. 수렴된 의견을 반영하여 규제개혁위원회 규제 심사 및 법제처 자문을 통해 2018년 11월 7일부로 '정보보호 및 개인정보 관리체계 인증 등에 관한 고시'가 시행되었다(박종승, 2020).

다음으로 '주요정보통신기반시설 기술적 취약점 분석평가 방법 상세가이드'는 악성코드 유포, 해킹 등과 같은 사이버 위협에 대한 취약점을 관리적, 물리적, 기술적 분야로 분석 및 평가하고 개선하는 제도로서 대상 기반시설의 정보보호 수준 향상을 그 목적으로 한다. 취약점 분석 및 평가를 위한 관리적 분야의 세부 점검항목 113개와 물리적 분야 18개, 기술적 분야의 세부 점검항목 347개로 구성되어 있다(김인환 外, 2017; 선종옥 外, 2021).

마지막으로 식약처에서는 2017년 11월에 의료기기 기술문서 및 허가·심사 시 제품의 특성에 따라 사이버 보안이 필요한 의료기기의 대상을 명확히 하고, 제조업체가 이에 대한 검증을 위해 제출해야 하는 자료의 범위를 정하여 유무선 네트워크 통신이 가능한 의료기기의 안전성을 확보하고자 '의료기기 사이버보안 가이드라인'을 발표하였다(식품의약품안전평가원, 2017; 김금현, 2019).

3) 조선·해운산업 정보보호 지침

선박 사이버보안은 일반적인 사이버보안과 별개의 개념이 아닌 일반적인 사이버보안에서 선박의 특수성을 반영한 선박과 관련된 ICT와 OT를 반영한 사이버보안의 개념으로 정의하고 있다(이은수, 2021).

항만 사이버보안의 실무자에 요청사항 중에는 항만시설에 대한 정보보호가 제대로 수행되지 않으면 항만 터미널에서 이루어진 물류서비스 체계가 정상동작 하지 않게 되며 이용자에게 근거를 제시할 수 없게 된다고 한다. 또한, 영업 및 전략 정보들이 경쟁관계의 회사에 노출된다면 경영에 있어 심각

8) ISMS-P : Personal information & Information Security Management System

한 문제에 놓일 수 있게 된다고 한다(이홍걸, 2007; DSLAB컴퍼니, 2021).

조선·해운산업과 관련된 국제기구 또는 해사협의회, 각 나라의 선급에서 발표된 사이버보안 지침과 발행연도(개정년도 포함)는 아래의 [표 2-1]과 같다.

[표 2-1] 해양 관련 사이버보안 지침 (연구자 구성, 2021)

기관	사이버보안 지침	발표년도
국제해사기구(IMO)	GUIDELINES ON MARITIME CYBER RISK MANAGEMENT	2017년
발틱국제해사협의회 (BIMCO)	THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS	2016년 (2017, 2019, 2020년 개정)
미국 선급(ABS)	CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES	2016년 (2021년 개정)
영국 선급(LR)	Introduction and Type Approval of Components within Cyber Enabled Systems	2015년
노르웨이 선급 (DNV)	Cyber security capabilities of systems and components	2018년 (2020년 개정)
프랑스 선급(BV)	Rules on Cyber Security for the Classification of Marine Units	2020년
일본 선급(NK)	ClassNK Cyber Security Approach	2019년

한국 선급(KR)	해상 사이버보안 시스템 지침	2018년 (2019, 2020, 2021년 개정)

제 3 절 조선·해운산업 사이버보안 침해사고

1) 조선산업 사이버보안 침해사고

가) GPS 전파교란(Jamming)

GPS 전파교란은 GPS 신호가 항법 위성에서 출발하여 지상 또는 선상의 수신 단말기에 도달할 때 다른 신호 발생원으로부터 전자파 간섭을 받아 GPS의 원 신호를 복조해내는 것이 매우 어렵거나 불가능해지도록 하는 것이다.

GPS 전파교란은 GPS 신호기와 노이즈 방출만으로 구분할 수 있다. 노이즈 방출은 기존 GPS 신호보다 강한 노이즈 신호를 방출하여 수신기가 GPS 신호를 정상적으로 수신하지 못하도록 방해하는 기법으로 재밍(Jamming)으로도 불린다. GPS 기만기법은 다시 미코닝(Meaconing)과 스푸핑(Spoofing)으로 구분된다. 미코닝은 재머(기만신호)의 위치를 자신의 현 위치로 착각하게 만드는 기법으로서 재머가 GPS신호를 수신하여 동 신호를 일정기간 지연시킨 후 재방출하는 교란 기법이다. 스푸핑은 수신기가 현 위치가 아닌 다른 위치로 착각하게 만드는 교란 기법으로서, GPS 신호를 수신 후 일부 조작하여 재방출하는 방법이다.

국내의 경우 2016년에 북한 소행으로 추정되는 GPS 전파교란으로 인한 어선의 해상좌표 시스템이 좌표를 찾지 못하는 장애가 발생되었다. 악의적인 목적으로 GPS 전파에 혼신을 일으켰으며 2010년부터 주로 을지연습, 독수리 훈련 등 국내 대규모 군사훈련 시기 동안에 발생되었다.

나) 잠수함 설계도 유출

2017년 4월에 북한이 국내조선소를 목표로 해킹하여 잠수함과 이지스함 등의 군함 설계도를 탈취한 것으로 확인되었다. 유출된 자료는 군사기밀 60여건, 일반 문건 4만 여건이 유출된 것으로 조사되었다. 안보전문가들은 '함정의 두뇌' 역할을 하는 전투체계 프로그램 제원과 성능, 지원 장비 등이 해킹당하여 우리 군의 해상수중 킬체인을 무력화를 노린 것으로 추정되는 만큼 관련 대응책 마련이 시급하다고 지적했다.

다) H선사 랜섬웨어 감염

H선사는 2019년 3월에 선박의 메인컴퓨터가 경찰청을 사칭한 이메일의 첨부파일로부터 랜섬웨어에 감염되어 피해를 입은 것으로 확인되었다. 랜섬웨어에 감염된 선박들은 해당 컴퓨터를 포맷하고 필요한 자료를 새로 작성하였다. 인터넷 접속이 가능한 메인컴퓨터엔 선박 입·출항에 필요한 수속서류와 운항에 필요한 자료가 담겨져 있어 피해가 있을 것으로 예상된다. 항만은 입·출항이 엄격하지만 항만에 진입하는 단계에서 이 같은 문제가 발생하였을 경우 본사뿐만 아니라 해당 항만이나 현지 업체 등과의 통신에 영향을 줄 수 있으며 이는 선박 운항에 심각한 차질을 초래할 수도 있다.

라) 컨테이너선박 항해시스템 사이버 공격

2017년 2월 키프로스에서 지부티까지 운항하는 독일 소유의 8,250TEU 컨테이너선박 항해시스템이 해킹되었다. 10시간 동안 선박 항해시스템이 완전히 장악당해서 사이버 해적이 조종을 할 수있게 되면서 특정 지역으로 선박이 이동하게 되었다. 선원은 항해시스템의 제어권한을 다시 얻으려 시도했지만 IT 전문가를 선내에 데려와서야 다시 작동할 수 있었다. 해커가 시스템에 침입한 경로는 불분명하지만 선박시스템이 사이버공격에 취약하고 악의적인 공격에 활용될 수 있음이 확인되었다.

마) Inmarsat 플랫폼 소프트웨어 취약점 확인

2017년 10월 Inmarsat Amos Connect 8.0 플랫폼에 심각한 소프트웨어 취약점이 확인되었다. SQL 인젝션 공격 및 원격 인증이 승인되지 않은 자가 AC 서버에서 임의의 코드를 실행할 수 있는 전체 시스템 권한을 제공하는 백도어 계정이 있었던 것으로 확인되었다. 이 결함을 이용하여 AmosConnect 서버에 저장된 중요한 정보에 대한 무단 네트워크 액세스를 얻고 잠재적으로 연결된 다른 시스템 또는 네트워크에 대한 접근 권한을 얻을 수 있다. Inmarsat AC에서 발견된 취약점은 CVE-2017-3221과 CVE-2017-3222로 CVE에 등록되었다. IOActive는 2016년 10월 Inmarsat에 취약점을 알렸고 2017년 7월 공개하였으며 시스템은 Inmarsat은 이후 AC 8.0 버전의 플랫폼을 2017년 6월에 서비스 종료하였다.

2) 해운산업 사이버보안 침해사고

가) 진도 VTS 해킹

2011년 3월 전남 진도 연안 해상교통관제센터(VTS[9])가 해킹으로 인해 서남해 연안의 국가 기간 레이더망 감시가 무력화되어 20일간 해당 해역을 통항하는 선박의 추적 및 감시, 관제 업무가 정상적으로 이루어지지 않은 사태가 발생했다. 사건 초기 송수신기와 안테나를 연결하는 연결케이블인 도파관 손상 등의 원인으로 인한 레이더 고장을 원인이라고 추정되어졌으나 사건일 전날 밤 외부와의 접촉이 없다는 점과 손상된 부분은 일반 절연 테이프로 연결해도 임시 사용이 가능한 점 등 외부 해킹에 무게가 실어졌다. 해양경찰청은 외부 접속의 흔적을 발견하여 이 흔적은 유지보수 업체 직원이 진도VTS와 네트워크가 연결된 완도 VTS를 통해 시스템에 장애를 일으켰다. 사고일 전후로 완도센터 컴퓨터 로그 파일과 출입기록, CCTV, 방문자 명단 기록부를 면밀히 조사하여 목표물의 추적과 정보 생성 등의 역할을 하는 레이더의

9) Vessel Traffic management System

기능인 'VET 기능'을 해킹으로 마비시킨 것으로 확인되었다.

나) 머스크라인 사이버 공격

2017년 6월에는 덴마크의 세계 최대 해운사 머스크라인는 전 세계 17군데의 머스크라인 소유의 항만 터미널 IT 시스템이 랜섬웨어 공격으로 피해가 발생하였다. 랜섬웨어 감염 경로는 직원의 송수신한 이메일을 통해 감염되었다. 3주간이나 컨테이너 선적작업이 수동으로 전환되었으며 총 피해규모는 3,000억 원으로 추산되었다. 4,000대 서버, 45,000대 PC, 2,500개의 Application이 재설치 되었다. 공격에 사용된 NotPetya 랜섬웨어는 항공 물류 운송업체 Fedex 시스템뿐만 아니라 우크라이나에 위치한 많은 기업을 대상으로 광범위한 피해를 입힌 이력을 가지고 있다고 분석되었다. NotPetya는 윈도우 SMB(Server Message Block) 취약점을 악용해 MBP(Master Boot Record) 파일 전체를 암호화해 복호화 비용으로 비트코일을 요구하는 랜섬웨어 'Petya'의 변종으로 윈도우 운영체제에서 동작하는 악성코드이다. Petya와 달리 NotPetya는 암호화된 데이터를 복구(복호화)하는 것이 원천적으로 불가능해 더욱 치명적인 것으로 나타났다.

다) BW 그룹, 사이버 해킹

2017년 7월에 유조선 등의 탱커선을 운영하는 BW 그룹은 회사 컴퓨터에 대한 무단 액세스로 인해 사이버공격이 발생했다고 전했다. BW Group은 KPMG의 사이버 보안 컨설팅을 도입하여 시스템에 대한 디지털 포렌식 감사를 실시했으며 랜섬웨어에 의한 것이 아님을 확인했다. 사이버공격은 BW그룹의 컴퓨터에 대한 비인가자의 무단 액세스로 액티브 디렉토리와 GPO 시스템에 영향을 미쳤으며 사이버공격으로 인해 BW그룹은 네트워크를 일시적으로 폐쇄시키는 상황으로까지 이어졌다.

라) 클락슨 내부자 사이버 범죄

2017년 12월 영국의 해운관련 통계분석서비스 회사인 Clarksonplc는 허가받지 않은 제3자가 영국의 회사 컴퓨터시스템에 무단 접근하여 데이터를 복사하고, 반환을 위해 몸값을 요구하는 사이버 보안 사건이 발생하였으며 그에 대한 세부사항을 공개했다. Clarksons는 2017년 11월 7일 위반사실을 알게 되었고 즉시 사건 대응 관리 및 조사를 위한 조치를 취했다. 허가받지 않은 제3자가 영국의 특정 Clarksons 컴퓨터시스템에 2017년 5월 31일부터 2017년 11월 4일 사이에 액세스하여 데이터를 복사하고 안전한 반환을 위해 돈을 요구했음이 디지털 포렌식 수사를 통해 밝혀졌다.

마) 샌디에고 항만 사이버 공격

샌디에고 항만 IT 시스템이 2018년 9월 25일 네트워크를 통한 침투공격에 당해 랜섬웨어 악성코드를 감염시키는 사이버공격을 받았다. 공격에 의해 항만 IT 시스템 중 일부가 손상되었으며 다른 시스템도 예방책으로 폐쇄되었다. 불과 일주일 전인 9월 20일 바르셀로나 항만 또한 랜섬웨어 사이버 공격을 받은 것으로 나타났으며 지난 7월 캘리포니아 롱비지항만의 COSCO 터미널이 랜섬웨어 공격을 받기도 했다. 2개월 만에 3개 항만이 사이버 공격을 받음으로써 의도적으로 사이버해킹 그룹이 항만을 표적으로 삼는 것으로 파악되고 있다.

바) 나이지리아 해킹 그룹 스피어피싱

2018년 4월에 선박 및 항만관리 서비스를 제공하는 회사를 포함하여 해운물류회사를 대상으로 사이버공격을 시도하는 나이지리아 Gold Galleon Hacking 그룹이 확인되었다. 2017년 6월에서 2018년 1월 사이에 해커가 3백 9십만 달러를 훔치려고 시도했으며 연간 6백 7십만 달러 도용을 시도한 것으로 추정된다.

Gold Galleon의 공격 전략과 기술은 신기술을 사용하거나 고급 기술을 사용하지 않지만 공격표적을 잘 선정하고 취약점을 이용한다. 그들은 실제 공격전에 회사 내 시스템에 침투해 선박일정, 대금 지불, 내부 및 거래처 연락처 등과 같은 관련 정보를 빼낸다. 그렇게 한 후 표적이 된 회사의 웹사이트를 면밀히 분석하여 사전 확보된 정보와 결합하여 사기에 이용한다. 즉 신뢰가 가는 이메일로 위장하여 스피어피싱 공격을 하는 것이다.

제 3 장 조선·해운산업 사이버보안 체계 연구

제 1 절 국제기구 사이버보안 지침

1) 국제해사기구(IMO)

국제해사기구(IMO)는 2017년에 “GUIDELINES ON MARITIME CYBER RISK MANAGEMENT”을 발표하였다. 이 지침은 해양 사이버 위험 관리에 대한 높은 수준의 권고사항을 제시하고 있으며, 운영상 사이버 위험에 탄력적인 안전하고 안전한 운송을 지원하기 위한 목적으로 국제해사기구가 제정한 안전 및 보안 관리 관행을 보완했다고 평가받고 있다.

IMO에서 정의한 사이버 기술은 해운의 안전과 보안 그리고 해양 환경의 보호에 중요한 요소이며 수많은 시스템의 운영과 관리에 필수적인 것으로 분류하였다. 이러한 시스템은 국제 표준 및 해당 관리 요건을 준수해야 함을 강조하였다. 사이버 위험으로부터 취약한 시스템으로는 교량 시스템, 화물 취급 및 관리 시스템, 추진 및 기계 관리 시스템, 전력 제어 시스템, 접근 제어 시스템, 승객 서비스 및 관리 시스템, 공공 네트워크를 공용하는 승객을 포함한 행정 및 승무원 복지 시스템, 통신 시스템 등 8개 시스템으로 구분하고 있다.

또한, IMO에서는 사이버 위험관리에 대해서도 매우 중요한 시점으로 접근하길 권고하고 있었다. 사이버 위험관리란 사이버 관련 위험을 식별 및 분석, 평가, 전달하고 이해관계자에게 취한 조치의 비용 및 편익을 고려하여 수용, 회피, 이전 또는 완화하는 과정을 의미한다. 지침에는 사이버 위험관리를 효과적으로 지원하는 기능적 요소를 제시하고 있다. 크게는 사이버 리스크 관리에 대한 인력 역할과 책임을 정의하고, 중단될 경우 배송 운영에 위험을 초래할 수 있는 시스템, 자산, 데이터 및 기능을 파악하는 식별, 위험 통제 프로세스 및 조치, 그리고 사이버 이벤트로부터 보호하고 운송 작업의 연속성을 보장하기 위한 비상 계획을 구현하는 보호,

사이버 사건을 적시에 탐지하는 데 필요한 활동을 개발하고 시행하는 탐지, 탄력성을 제공하고 사이버 이벤트로 인해 손상된 운송 운영 또는 서비스에 필요한 시스템을 복구하기 위한 활동 및 계획을 개발하고 구현하는 응답, 사이버 이벤트의 영향을 받는 배송 운영에 필요한 사이버 시스템을 백업 및 복원하기 위한 조치를 식별하는 복구 5가지로 나눌 수 있다. 이 구분은 미국 국립 표준 기술 연구소(NIST, National Institute of Standards and Technology)의 중요 인프라 사이버 보안 개선을 위한 프레임워크를 참조하고 있다. 각 요소에 대한 23개의 항목과 108개의 세부 항목으로 이루어져 있으며 주요 기능별 카테고리는 아래의 [표 3-1]과 같이 구분되어 진다.

[표 3-1] NIST 사이버보안 프레임워크(NIST, 2018)

기능	카테고리	세부 카테고리
IDENTIFY (ID)	자산 관리(ID.AM): 조직이 비즈니스 목적을 달성할 수 있도록 하는 데이터 및 인력, 장치, 시스템, 시설은 조직 목표 및 조직의 위험 전략에 대한 상대적 중요성에 따라 식별 및 관리	6
	비즈니스 환경(ID.BE): 조직의 사명, 목표, 이해 관계자 및 활동을 이해하고 우선 순위를 지정합니다. 이 정보는 사이버 보안 역할 및 책임, 위험 관리 결정을 알리는 데 사용	5
	거버넌스(ID.GV): 조직의 규제 및 법적, 위험, 환경, 운영 요구 사항을 관리 및 모니터링하기 위한 정책 및 절차, 프로세스를 이해하고 사이버 보안 위험 관리에 알림	4
	위험 평가(ID.RA): 조직은 조직 운영(임무 또는 기능, 이미지, 평판 포함), 조직 자산 및 개인에 대한 사이버 보안 위험을 파악	6
	위험 관리 전략(ID.RM): 조직의 우선 순위 및 제약 조건, 위험 허용 범위, 가정이 설정되어 운영 위험 결정을 지원하는 데 사용	3

	공급망 위험 관리(ID.SC): 조직의 우선 순위 및 제약 조건, 위험 허용 범위, 가정이 설정되고 공급망 위험 관리와 관련된 위험 결정을 지원하는 데 사용됩니다. 조직은 공급망 위험을 식별 및 평가, 관리하기 위한 프로세스를 수립하고 구현	5
PROTECT (PR)	ID 관리 및 인증, 액세스 제어(PR.AC): 물리적 및 논리적 자산 및 관련 시설에 대한 액세스는 승인된 사용자 및 프로세스, 장치로 제한되며 승인된 활동 및 트랜잭션에 대한 승인되지 않은 액세스의 평가된 위험과 일관되게 관리	7
	인식 및 교육(PR.AT): 조직의 직원 및 파트너에게 사이버 보안 인식 교육을 제공하고 관련 정책 및 절차, 계약에 따라 사이버 보안 관련 의무 및 책임을 수행하도록 교육	5
	데이터 보안(PR.DS): 정보 및 기록(데이터)은 정보의 기밀성 및 무결성, 가용성을 보호하기 위해 조직의 위험 전략에 따라 관리	8
	정보 보호 프로세스 및 절차(PR.IP): 정보 시스템 및 자산 보호를 관리하기 위해 보안 정책(목적 및 범위, 역할, 책임, 관리 약속, 조직 엔티티 간의 조정), 프로세스 및 절차를 유지 관리하고 사용	12
	유지보수(PR.MA): 산업 제어 및 정보 시스템 구성요소의 유지보수 및 수리는 정책 및 절차에 따라 수행	2
	보호 기술(PR.PT): 기술 보안 솔루션은 관련 정책, 절차 및 계약에 따라 시스템 및 자산의 보안 및 복원력을 보장하기 위해 관리	5
DETECT (DE)	변칙 및 이벤트(DE.AE): 변칙 활동이 감지되고 이벤트의 잠재적 영향을 파악	5
	보안 연속 모니터링(DE.CM): 사이버 보안 이벤트를 식별하고 보호 조치의 효과를 확인하기 위해 정보 시스템 및 자산을 모니터링	8

	탐지 프로세스(DE.DP): 탐지 프로세스 및 절차를 유지 관리하고 테스트하여 비정상적인 이벤트를 인식	5
RESPOND (RS)	대응 계획(RS.RP): 탐지된 사이버 보안 사고에 대한 대응을 보장하기 위해 대응 프로세스 및 절차가 실행 및 유지	1
	커뮤니케이션(RS.CO): 대응 활동은 내부 및 외부 이해 관계자와 조정 (예: 법 집행 기관의 외부 지원).	5
	분석(RS.AN): 효과적인 대응을 보장하고 복구 활동을 지원하기 위해 분석을 수행	5
	완화(RS.MI): 이벤트의 확장을 방지하고 그 영향을 완화하며 사고를 해결하기 위한 활동을 수행	3
	개선(RS.IM): 조직의 대응 활동은 현재 및 이전의 탐지/대응 활동에서 얻은 교훈을 통합하여 개선	2
RECOVER (RC)	복구 계획(RC.RP): 사이버 보안 사고의 영향을 받는 시스템 또는 자산의 복원을 보장하기 위해 복구 프로세스 및 절차가 실행되고 유지	1
	개선(RC.IM): 학습한 교훈을 미래 활동에 통합하여 복구 계획 및 프로세스를 개선	2
	커뮤니케이션(RC.CO): 복구 활동은 내부 및 외부 당사자(예: 조정 센터, 인터넷 서비스 제공업체, 공격 시스템 소유자, 피해자, 기타 CSIRT 및 공급업체)와 조정	3

2) 발틱국제해사협의회(BIMCO)

발틱국제해사협의회(BIMCO)는 선박에 관한 사이버보안 지침인 “THE

GUIDELINES ON CYBER SECURITY ONBOARD SHIPS"을 2016년 최초 발표 이후 2020년까지 3차례에 걸쳐 개정안을 공표 하였다. 여기서 정의한 사이버 보안은 "인력, 선박, 환경, 회사, 화물에 미치는 잠재적 영향이 부정적으로 적용되는 것을 통제하기 위해 IT, OT, 정보 및 데이터를 무단 액세스하여 조작하게 되는 행위 및 서비스 중단으로부터 보호"하는 것으로 정의하고 있다. 조선·해운산업에서 데이터 분석, 스마트 선박 및 산업 사물 인터넷(IIoT)의 사용이 증가함에 따라 위협 행위자와 잠재적인 공격이 증가할 것으로 우려되고 있다. 사이버 위험 관리는 선박의 안전하고 효율적인 운항을 위해 기업 안전·보안 문화의 본질적인 부분이 되어야 하며 육상의 고위 경영진과 선상 인력 등 회사 각급에서 사이버보안을 위해 사이버 위험 관리를 수행해야 한다.

아래의 [그림 3-1]은 사이버 위험 관리 접근법으로 위험 식별, 취약점 식별, 위험 노출 평가, 보호 및 탐지 대책 개발, 대응 계획 수립, 사이버 보안사고 대응 및 복구의 6단계 과정을 나타내고 있다. 먼저 위협 식별은 선박에 대한 외부 사이버 보안 위협과 부적절한 사용이나 열악한 사이버 보안 관행으로 인해 발생하는 내부 사이버 보안 위협을 이해하는 단계이다. 취약점 식별 단계는 직접 및 간접 통신 링크가 있는 온보드 시스템에 대한 사이버 보안 위협의 결과를 이해해야 한다. 위험 노출 평가는 외부 위협에 의해 취약성이 악용될 가능성을 파악하고 부적절한 사용으로 인해 취약성이 노출될 가능성을 파악하여 악용되는 개별 또는 취약성 조합의 보안 및 안전 영향을 확인하는 단계이다. 보호 및 탐지 대책 개발 단계를 통해 취약성이 악용될 가능성을 줄이고 취약성이 악용될 경우 발생할 수 있는 영향을 줄인다. 확인된 사이버 위험에 효과적으로 대응하기 위한 대응 계획 수립단계를 통해 사이버 보안사고 대응 및 복구하고 대응 계획 효과의 영향을 평가하고 위협 및 취약성을 재평가 한다(BIMCO. 2020).

[그림 3-1] 사이버 위험 관리 접근 방식 6단계 (BIMCO, 2020)

사이버 위험 관리 접근법 6단계는 위협식별, 취약점 식별, 위험 노출 평가, 보호 및 탐지 대책 개발, 대응계획 수립, 사이버 보안사고 대응 및 복구와 같으며 상세 내용은 아래의 [표 3-2]와 같다.

[표 3-2] 사이버 위험 접근 방식(BIMCO, 2020)

Function	Category
위협 식별	위협 행위자
	사이버 위협의 유형

	사이버 사건의 단계
	위협 정량화
취약점 식별	일반적인 취약점
	IT 및 OT시스템 문서
	일반적인 취약 시스템
	선박과 해안 간 인터페이스
	선박 방문
	원격 액세스
	시스템 및 소프트웨어 유지보수
위험 노출 평가	위협과 취약성의 산물로서의 가능성
	가능성 정량화
	CIA 모델
	영향 정량화
	주요 장비 및 기술 시스템
	위험에 영향을 미치는 요인간의 관계
	위험 평가의 4단계
	제3자 위험 평가
보호 및 탐지 대책 개발	깊이 있고 폭 넓은 방어
	기술적 보호 조치
	절차적 보호 조치
	탐지 및 차단, 경고
	멀웨어 탐지
대응 계획 수립	비상 계획 수립
사이버 보안 사고 대응 및 복구	효과적인 대응
	사고 대응의 4단계
	데이터 복구 기능 사이버 사건 수사
	사이버사고로 인한 손실

제 2 절 해외선급협회 사이버보안 지침

1) 미국 선급(ABS)

미국 선급(ABS)[10]은 2016년에 해양 및 해양 산업을 위한 사이버 보안 구현 가이드라인을 공개하고 2021년 개정된 지침을 공개하였다. 이 가이드라인에는 조직 관리 시스템 프로세스 및 비즈니스 규칙이 지원하는 구현된 기술 사이버보안 보호 메커니즘 및 통제사항 검증에 대한 ABS 접근방식이 제시되어 있다. 검증은 관련 문서를 검토하고 선박 내 조사를 수행할 것을 명시하고 있다.

Classification Scope(CS)는 아래의 [표 3-3]와 같이 CS-System와 CS-Ready, CS-1, CS-2 4개의 등급으로 구분된다. CS-System 및 CS-Ready는 OEM에 의한 사이버 지원 제품 제조 및 조선업체/통합업체의 사이버 지원 선박 건조 중 사이버 보안 보호 및 절차의 적용 및 문서화를 요구하며, CS-1 및 CS-2에서는 소유자와 운영자가 문서화된 조직 및 선박별 사이버 보안 절차와 보호를 포함하는 사이버 보안 프로그램을 수립하여 사이버 지원 시스템에 대한 위험을 최소화하고 관리할 것을 명시하고 있다.

[표 3-3] CS 표기법 적용 가능성(ABS, 2021)

구분	적용 대상	목적
CS-System	Original Equipment Manufacturer (OEM) equipment installed on a specified vessel	Notation documents that at least one of the installed systems, providing a Primary Essential Service, has an active ABS CyberSafety PDA Certificate per 2/1.1 of this Guide. This notation provides OT/IT system information that can be utilized by the Company to satisfy certain CS-1 and CS-2 requirements.
CS-Ready	Ship Builder	Notation documents that

10) ABS : American Bureau of Shipping

	Integrator (SBI) applied to a specified vessel	cybersecurity procedures and protections are applied to critical OT/IT systems during vessel construction and are documented and communicated to the Owner per 2/1.2 of this Guide. This notation provides OT/IT system information that can be utilized by the Company to satisfy certain CS-1 and CS-2 requirements.
CS-1 / CS-2	Company, Owner, or Vessel Manager applied to a specified vessel	Notation documents that the vessel has met requirements for a cybersecurity program per 2/1.3 of this Guide.

또, 미국 선급(ABS)은 2021년에 IMO의 사이버 위험 관리 지침에 대한 입문서를 발간하였다. 이 입문서에는 사이버 위협이 빠른 속도로 성장하며 치명적으로 다가옴에 따라 안전한 운항과 시스템 운영 및 관리를 위해 사이버 기술은 필수 불가결하게 되었다. 그렇기 때문에 사이버 위협으로 부터 안전과 방지를 위하고 Cyber Risk Management를 구축하기 위해 정보기술(IT), 기술시스템(OT) 뿐만 아니라 물리적 보안까지 보호 및 탐지 계층을 넓히도록 권장하고 있다. 미국 선급(ABS)에서는 조직과 직원의 사이버 보안 규율 및 능력 미숙으로 인한 인적 오류가 발생함에 따라 정보보안 인식을 강화하기 위한 대책이 필요해 졌다. 이에 따라 보안사고 예방 및 대책 방안을 수립하고 교육할 것을 강조하고 있다.

2) 영국 선급(LR)

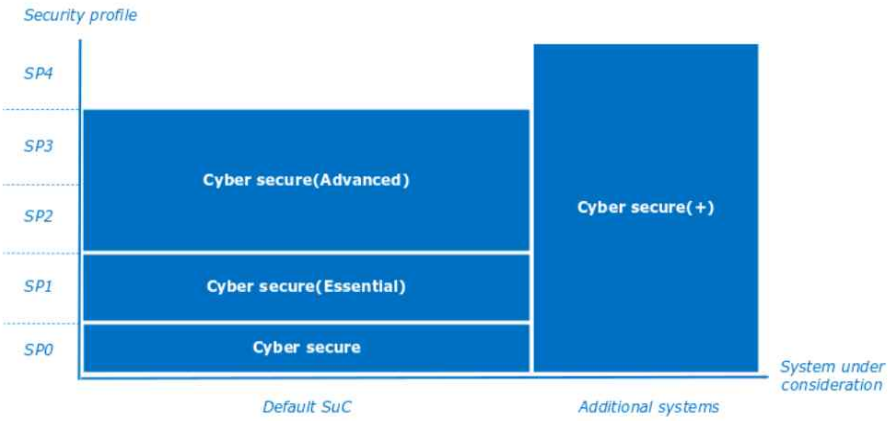
영국 선급인 Lloyd's Register(LR)에서는 선급에서 독자적인 사이버보안 지침은 없으나 2017년에 공개한 “Introduction and Type Approval of Components within Cyber Enabled Systems”에 따르면 LR은 잠재적인 사이버 보안 이벤트에 대한 시스템과 자산의 사이버 보안 복원력 평가에 NIST 프레임워크의 식별(Identify), 보호(Protect), 탐지(Detect), 대응

(Respond), 복구(Recover)의 다섯 가지 핵심 기능을 사용하는 것으로 발표하였다(LR, 2017).

그리고 2018년에 공개한 “LR approach to cyber security”에서는 BIMCO의 사이버 위험 관리 접근 방식의 각 단계에 대해 지침을 제시하고 있다. 먼저 위협 식별은 선박과 항만이 자동화되고 상호연결 기술 발전에 따른 사이버 취약성 증가와 잠재적 손실 증가되는 환경에서 Cyber Attack Lifecycle이 정보 수집, 익스플로잇 이용, 멀웨어 실행, 채널 제어, 데이터 유출의 단계를 거쳐 진행된다고 나타내고 있다. 다음으로 취약성 식별은 선박자동식별시스템(AIS, Automatic Identification System) 및 전자해도정보시스템(ECDIS, Electronic Chart Display and Information System), 위성항법시스템(GPS)을 예로 들고 있다. 위험 평가 단계에서는 온보드 상의 IT 및 OT 시스템을 보호하기 위한 기존 기술 및 절차 제어를 바탕으로 하여 취약한 IT 및 OT 시스템을 식별하고 식별된 취약성이 미치는 영향을 고려하여 완화조치의 우선순위를 정하는 일련의 위험의 영향 및 발생 가능성을 식별하는 과정이다. 비상대책 단계에서는 비상 사태 발생 시 중요한 IT 서비스를 지속하고 복구하기 위한 활동으로 IT 시스템에 대한 위험을 식별 및 이해, 정량화, 완화 하는 과정이 포함되며 연방정보 시스템을 위한 비상 계획 가이드인 NIST SP800-34의 비상계획 7단계는 비상 계획 정책 개발, 비즈니스 영향 분석, 예방 통제 식별, 복구 전략 개발, 비상 계획 개발, 테스트 훈련 및 연습 계획, 유지보수 계획으로 이루어져 있다. 마지막으로 대응 및 복구 단계에서 보유하고 있는 중요 자산과 데이터를 식별, 사고 발생 시 조직이 취해야 할 단계를 개략적으로 설명하는 계획을 수립, 사고 대응 계획에 대한 테스트 수행, 긴급구조대 기능을 개발할 수 있도록 교육을 받은 직원이 있는지 확인, 사고 대응 활동을 수행할 수 있도록 기술 인력을 교육하거나 이러한 기능에 신속하게 액세스할 수 있도록 해야 한다고 나타내고 있다.

3) 노르웨이 선급(DNV)

Det Norske Veritas(DNV)는 노르웨이의 선급으로 아래의 [그림 3-2]와 같이 보안 등급 구분하기 위해 Secure Profile(SP)은 요구 사항의 선택을 그들의 필요에 맞게 조정하기 위해 다양한 산업/그룹 부문 또는 조직을 위한 것으로 SP0부터 SP4까지 5개로 분류하였다. '검토 중인 시스템(SuC)'이라는 표현은 사이버 보안 프로젝트에서 고려되어야 하는 모든 사이버 물리 시스템을 총칭하는 용어이다. SP와 SuC의 관계를 고려하여 보안등급을 사이버 보안 등급을 4개로 구분하고 있다. Cyber Secure는 SP0의 요구사항을 따르며 Cyber Secure(Essential)은 SP1의 요구사항을 따른다. Cyber Secure (Advanced)는 SP3의 요구사항을 따르게 되며 Cyber Secure(+)는 고려중인 시스템과 위험 감소 수준에 대한 유연성을 제공하는 것으로 같이 쓰이는 Cyber Secure의 SP 요구사항의 수준을 높일 수 있다(DNV, 2021).



[그림 3-2] 사이버보안 등급 표기법(DNV, 2021)

Security profile의 요구사항 IEC 62443의 보안 수준을 따르며 SP0은 위험 감소의 초기 수준을 제공하며 SP1은 IEC 62443 보안 수준 1을 기반으로 하며 일반적인 사이버 위협에 대한 보호를 제공한다. SP2는 IEC 62443 보안 수준 2를 기반으로 하여 자원 및 동기부여가 낮은 위협행위자의 고의침해로부터 보호하는 수준이다. SP3은 보안 수준 3을 기반으로 중간 정도의 자원과

특정 OT시스템 기술을 보유한 위협 행위자에 의한 고의적인 침해로부터 보호해야 한다. SP4는 IEC 62443 보안 수준 4를 기반으로 하며 확장 자원, 높은 동기 부여 및 특정 OT 시스템 기술을 보유한 위협 행위자에 의한 의도적인 위반에 대한 보호를 제공해야 할 것을 강조하고 있다(DNV, 2021).

4) 프랑스 선급(BV)

프랑스 선급인 Bureau Veritas(BV)는 해상부대분류 사이버보안 규칙을 2018년에 발표하였다. 이 규칙은 아래의 [표 3-4]와 같이 크게 7개의 General Principles, Additional Class Notation CYBER MANAGED PREPARED, Additional Class Notation CYBER MANAGED, Additional class notation CYBER SECURE PREPARED, Additional class notation CYBER SECURE, Type approval equipment, Survey Operations로 구분하고, 22개의 카테고리와 192개의 세부항목을 포함하고 있다.

[표 3-4] 해상분류의 사이보보안 규칙(BV, 2020)

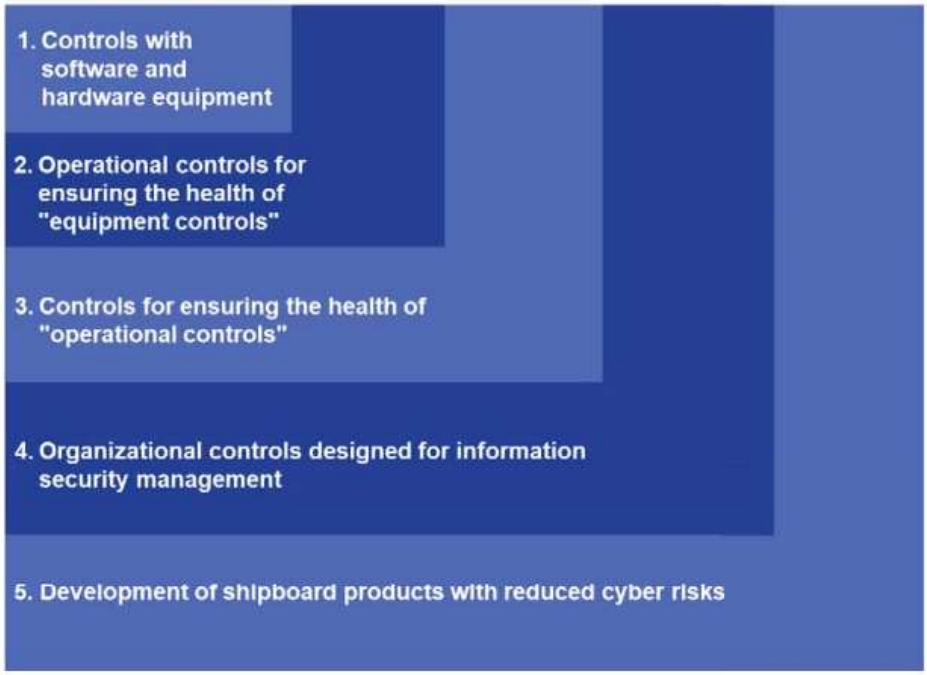
구분	카테고리	세부항목
General Principles	General Requirements	12
	Cyber Repository	15
	Criticality Assessment	15
	Design Assessment	13
	Risk Assessment	13
	Cyber Handbook	10
Additional Class Notation CYBER MANAGED PREPARED	Cyber Managed Prepared Class	3
Additional Class	Cyber Managed Class	3

Notation CYBER MANAGED	Cyber Security Policy	15
Additional class notation CYBER SECURE PREPARED	Cyber Secure Prepared Class	3
	On board to On shore Connections	7
	Vessel Networks	6
	Operation Technologies Interconnections	4
Additionalclassnotation CYBERSECURE	Cyber Secure Class	3
Type approval equipment	Type Approval Certificate	3
	Equipment Design	24
	Security Solutions	13
Survey Operations	General	6
	Monitoring Survey	6
	Infrastructure Survey	7
	Equipment Survey	6
	Maintenance Procedures Survey	5

5) 일본 선급(NK)

일본 선급 NIPPON KAIJI KYOKAI(NK 또는 ClassNK)는 사이버보안 제어를 아래의 [그림3-3]과 같이 1계층부터 5계층으로 구분하고 있으며, 1계층은 소프트웨어 및 하드웨어 장비로 제어, 2계층은 "장비 제어"의 상태 유지를 위한 운영 통제, 3계층은 "운영 통제"의 상태 보장을 위한 조치, 4계층은 정보 보안 관리를 위해 설계된 통합 제어, 마지막으로 5계층

은 사이버 리스크 감소 선상제품 개발로 정의하고 있다(NK, 2019).



[그림 3-3] 사이버 보안 제어 계층(NK, 2019)

ClassNK 사이버 보안 시리즈에는 사이버 보안 선상 설계 지침과 선박용 사이버보안 관리 시스템, 소프트웨어 보안 지침이 있다. 먼저, 사이버 보안 선상 설계 지침은 조선소와 선주를 대상으로 NIST SP800-82를 참조하여 NIST SP800-53의 선박에 적용되는 통제항목을 선별하고 이는 1계층과 2계층, 3계층이 해당된다. 그리고 선박용 사이버 보안 관리 시스템은 4계층이 해당되며 선박관리회사와 선박을 대상으로 ISO 27001 및 ISO 27002의 기본 구조를 사용하는 ISM 코드 시스템과의 호환성을 목표로 관리한다. 마지막으로 5계층이 해당되는 소프트웨어 보안 지침은 선상장비 제조업체를 대상으로 ISO/IEC 표준에서 추출한 선박에 필요한 요소를 갖춘 지침에 따라 개발 프로세스 및 기능 요구사항을 확인할 것을 권고하고 있다(NK, 2019).

제 3 절 한국 선급 사이버보안 지침

우리나라의 국적선급인 한국선급(KR)은 해사 사이버보안 시스템 지침을 2018년 발표하였고 최근에는 2021년에 개정된 가이드라인을 발표하였다.

[표 3-5] 사이버보안 수준에 따른 선박 등급표(한국선급, 2021)

구분	대상 선박	내용
CS Ready	사이버보안 시스템을 갖춘 신조선	사이버보안 시스템 준수를 위한 IT/OT 영역 내 사이버보안 관련 필수 요건
CS1	기존 사이버보안 시스템을 운용 중인 선박	기본적인 정책 및 절차 보유, 사이버보안 관리 시스템의 부분적 구현, 사이버 위협 최소한 대응 가능
CS2	향상된 사이버보안 시스템을 운용 중인 선박	사이버보안 조직 운영, 지속적인 사이버 리스크 관리 활동, 사이버보안 관리 시스템의 대부분 구현, 대부분의 사이버 위협 대응 가능
CS3	고등 사이버보안 시스템을 운용중인 선박	사이버 위협 예방 가능, 침해 사고 발생 시 빠른 대응 및 복구 가능, 지속적으로 사이버보안 관리 시스템 향상

선박의 패러다임이 변화하면서 선박과 회사에 ICT와 OT 시스템에 대한 사이버보안의 중요성이 증가하였다. 한국 선급의 해사 사이버보안 지침에 해당하는 대상은 선박 및 회사와 조직·정책·프로세스, 리스크 관리, 상세 사이버보안 활동을 대상으로 한다. 상기의 [표 3-5]는 해사 사이버보안 등급은 CS Ready와 CS1(Basic), CS2(Enhanced), CS3(Advanced) 4개의 등급으로 구분된다(한국선급, 2021).

CS-Ready 등급의 선박에 대한 사이버보안 지침은 13개의 지침항목과 50개의 세부 지침 항목이 해당되며 아래에 기술된 [표 3-6]과 같이 지침항목과 지침에 대한 내용 및 세부 지침 개수로 나열된다.

[표 3-6] CS-Ready 등급의 선박 사이버보안 지침(한국선급, 2021)

지침항목	지침 내용	세부 지침 개수
리스크 관리	선박 내 IT 및 OT에 영향을 미칠 수 있는 리스크를 식별하고 관리에 대한 절차 수립 및 수행	5
자산 관리	보호되어야 하는 모든 자산(시스템, 설비, 데이터 등)을 분류하여 문서화	1
접근 통제	시스템에 접근하는 사용자의 권한을 최소화 및 명확화 하여 접근을 제한	3
물리적 보안	보호구역에 대한 접근 제한과 주요 시스템에 대한 물리적 위험으로부터의 보안	5
사고대응 및 복구	비상상황 발생 시에도 선박 내 운영 시스템이 운영될 수 있도록 대응 및 복구에 대한 절차	2
데이터 보안	데이터에 대한 접근통제와 암호화 등을 통해 보호	4
로그 관리	시스템 별 로그를 일정 기간 동안 관리하기 위한 절차	5
시스템 관리	시스템 내 보안설정과 하드웨어·소프트웨어 변경사항을 관리	7
패치 관리	선박 내 시스템의 패치에 대한 취약성 및 장애요인 등을 사전 확인 후 패치하도록 관리	3
악성코드 대응	악성코드로부터 시스템을 보호	1

네트워크 관리	내·외부 네트워크에 대한 접근 통제 및 관리에 대한 지침	10
소프트웨어 품질 관리	선박 내 시스템에 설치되는 소프트웨어의 품질에 대한 관리 절차	2
사이버보안 시험	사이버보안 기능에 대한 보안 요구사항과 평가	2

CS1(Basic) 등급의 선박에 대한 사이버보안 지침은 18개의 지침항목과 81개의 세부 지침 항목이 해당되며 아래의 [표 3-7]과 같이 지침항목과 지침에 대한 내용 및 세부 지침 개수로 나열된다.

[표 3-7] CS1(Basic) 등급의 선박 사이버보안 지침(한국선급, 2021)

지침항목	지침 내용	세부 지침 개수
사례 검토	사이버보안 위협, 사례 등의 정보를 선원들에게 공유	1
보안 정책	보안 운영을 위한 운영방법, 절차, 책임자 등을 명시한 사이버보안 정책서를 마련 및 관리	2
보안 교육	연 1회 이상 보안교육 계획에 따라 승선자와 하선자, IT/OT 운영인력에게 보안교육 실시	3
리스크 관리	선박 내 IT 및 OT에 영향을 미칠 수 있는 리스크를 식별하고 관리에 대한 절차 수립 및 수행	6
자산 관리	보호되어야 하는 모든 자산(시스템, 설비, 데이터 등)을 분류하여 문서화	4
접근 통제	시스템에 접근하는 사용자의 권한을 최소화 및 명확화 하여 접근을 제한	7

물리적 보안	보호구역에 대한 접근 제한과 주요 시스템에 대한 물리적 위험으로부터의 보안	11
사고대응 및 복구	비상상황 발생 시에도 선박 내 운영 시스템이 운영될 수 있도록 대응 및 복구에 대한 절차	5
외부자 보안	외부자의 접근에 대한 보안 정책서 및 책임자의 승인 절차	3
데이터 보안	데이터에 대한 접근통제와 암호화 등을 통해 보호	4
로그 관리	시스템 별 로그를 일정 기간 동안 관리하기 위한 절차	5
시스템 관리	시스템 내 보안설정과 하드웨어·소프트웨어 변경사항을 관리	7
패치 관리	선박 내 시스템의 패치에 대한 취약성 및 장애요인 등을 사전 확인 후 패치하도록 관리	3
모바일 보안	선박 내 모든 모바일 기기의 식별 및 관리, 통신 제한, 촬영 제한 등	4
암호화	데이터 보호를 위한 암호화 적용	3
악성코드 대응	악성코드로부터 시스템을 보호	1
네트워크 보안	내·외부 네트워크에 대한 접근 통제 및 관리에 대한 지침	10
사이버보안 내부심사	정책 위반사항을 내부 심사계획에 따라 보고하고 주기적으로 보안 실태 점검 및 교육 실시	2

CS2(Enhanced) 등급의 선박에 대한 사이버보안 지침은 9개의 지침항목과 28개의 세부 지침 항목이 해당되며 아래에 기술된 [표 3-8]과 같이 지침항목과 지침에 대한 내용 및 세부 지침 개수로 나열된다.

[표 3-8] CS2(Enhanced) 등급의 선박 사이버보안 지침(한국선급, 2021)

지침항목	지침 내용	세부 지침 개수
위협정보 수집체계 구축	사이버보안 위협, 사례 등을 검토하여 선박 정책에 반영	1
보안 정책 및 매뉴얼의 지속적 관리	사이버보안 지침 및 매뉴얼의 주기적 검토를 통해 국제기구의 요구사항을 반영하고 개정사항 관리	2
전문 보안 교육	내·외부 환경요인, 자산 변경 등을 고려한 강화된 보안 교육 계획 수립	1
이상 징후 탐지	시스템에 대한 비인가자의 접속 또는 이상 징후 탐지 기능 보유	5
선박 내 물리적 통제 개선	보호구역 내 설치된 CCTV의 주기적 검사 및 통신망 분리	2
침해사고 대응 역량 강화	사고의 유형별로 분류하고 사고 대응 절차서를 수립, 침해사고 조사 분석, 모의훈련(침투테스트 등)을 통한 역량 강화	12
모바일 보안관리	기술적 보안을 적용한 모바일 기기 사용통제	1
변경관리	시스템 별 변경이력 관리 및 영향도, 예상 장애 등의 사전 테스트 수행	2

비즈니스 연속성 강화	리스크 관리 프로세스와 연계된 비즈니스 연속성 유지를 위한 시스템 운영매뉴얼 수립	2

CS3(Advanced) 등급의 선박에 대한 사이버보안 지침은 6개의 지침항목과 15개의 세부 지침 항목이 해당되며 아래의 [표 3-9]와 같이 지침항목과 지침에 대한 내용 및 세부 지침 개수로 나열된다.

[표 3-9] CS3(Advanced) 등급의 선박 사이버보안 지침(한국선급, 2021)

구분	지침항목	세부 지침 개수
보안체계의 일원화	유관된 법률, 표준, 기술 가이드 등을 선박 정책에 반영	1
보안엔지니어링	보안 관련 이슈사항을 주기적으로 테스트하는 훈련을 실시	1
비즈니스 연속성 보장	내·외부 환경요인과 자산 변경 등을 고려한 사고대응 계획 수립 및 재해복구를 위한 보안요구사항 적용, 모의훈련 실시	7
실시간 모니터링 역량 강화	네트워크 트래픽을 실시간 모니터링하여 비정상적인 통신을 감시하고 제한조치를 실행	3
사이버보안 심사	사이버보안 전문기관에 의한 사이버보안 심사에 관한 정책서 비치, 검토, 관리	2
암호키 관리	암호키는 절차를 수립하여 관리, 접근통제 정책에 따라 분리 보관	1

제 4 절 사이버보안 관리체계 개선방안

Panam Choi & Seungwhoon Han(2015)의 연구에서는 기업정보보호활동의 개념은 최근 산업기밀 유출의 심각성에도 불구하고 국내에서는 아직까지 명확하게 정의되어 있지 않지만, 관리적 요인과 기술적 요인, 시스템적 요인으로 분류(Holmes, 2001이상준, 2008; 한국정보사회진흥원, 2008; 행정안전부, 2008; 정구헌, 2011)되고 있으며 현재 기업의 입장에서 인적자원, 정보, 물리적 자산을 보호하고 회사 정보자산의 위험을 감소시키는 제반활동으로 정의(노민선·이삼열, 2010)하고 있다. 관리적 요인은 기업정보보호를 위해 수립된 정보보호 요인에 근거하여 적절하게 관리되고 있는지를 확인하는 통제활동(박태완, 1997)을 의미하며 기술적 요인은 시스템 보안과 네트워크 보안 분야의 광범위한 내용을 이야기 하고 있다(Post & Kagan, 2000). 그리고 조직 내 지역을 제한구역과 통제구역으로 구분하고 출입하는 인원, 정보시스템 및 전산장비의 사용, 반출, 반입에 대해 관리 수단을 차등을 두어 통제하는 것을 시스템적 요인으로 이야기 한다(Solms, 2001).

정보보안 인식과 정책, 지침과 관련된 침해사고를 관리적 보안 문제로 구분하였다. 그리고 시스템 및 네트워크와 관련된 침해사고를 기술적 보안 문제로 구분하였다. 또한 제한구역 또는 통제구역으로의 출입, 정보통신기기 반출·입과 관련된 보안문제를 물리적 보안 문제로 구분하였다.

조선·산업분야에서 발생한 사이버보안 침해사고들의 원인 유형은 랜섬웨어 악성코드 감염과 기밀문서·중요정보 유출, 비인가자의 시스템 접근을 이용한 장애발생으로 분석될 수 있다. 사례들을 분석한 결과 아래에 기술된 [표 3-10]과 같이 분류할 수 있었으며 유형별로는 관리적 보안 문제로 구분된 침해사고 사례가 4건이 있었고 기술적 보안 문제로 구분된 침해사고 사례는 7건으로 집계되었다. 그러나 물리적 보안 사고로 분류된 침해사고 사례는 한차례도 없었다고 보도 되었다.

[표 3-10] 해사 사이버보안 침해사고 원인 유형 분석(연구자 재구성, 2021)

침해사고	침해사고 원인	원인 유형
GPS 전파교란	GPS 전파 신호를 악의적으로 교란시켜 GPS 전파 혼신	기술적 보안 문제
잠수함 설계도 유출	해킹을 통한 군사기밀 및 자료 유출	기술적 보안 문제
H선사 랜섬웨어 감염	경찰청을 사칭한 이메일의 첨부파일을 통한 랜섬웨어 감염	관리적 보안 문제
컨테이너선박 항해시스템 사이버 공격	해커에 의해 항해시스템이 장악되어 제어권 상실	기술적 보안 문제
Inmarsat 플랫폼 소프트웨어 취약점 확인	Amos Connect 8.0 버전의 플랫폼에서 취약점이 발견	기술적 보안 문제
진도 VTS 해킹	유지보수 업체 직원이 완도VTS에서 네트워크를 통해 진도VTS 시스템에 장애를 일으킨 내부자 해킹	관리적 보안 문제
머스크라인 사이버 공격	직원의 이메일 송수신 과정에서 랜섬웨어 감염 시작(근거필요)으로 보안의식 부족에 의한 인적 보안 사고	관리적 보안 문제
BW 그룹 사이버 해킹	승인되지 않은 외부의 무단 액세스로 액티브 디렉토리와 GPO 시스템이 영향을 받았고 문제는 인터넷과 인트라넷 시스템을 일시적으로 폐쇄	기술적 보안 문제
클락슨 내부자 사이버 범죄	승인되지 않은 제3자가 컴퓨터 시스템에 무단 액세스하여 데이터 유출	기술적 보안 문제

샌디에고 항만 사이버 공격	랜섬웨어 악성코드가 네트워크를 통해 침투해 관리 시스템 장애 발생	기술적 보안 문제
나이지리아 해킹 그룹 스피어피싱	이메일을 통한 스피어피싱 공격	관리적 보안 문제

침해사고 원인에 대한 분석을 통해 관리적, 기술적 보안 문제인 것으로 분석되며 침해사고 유형과 같이 이메일을 통한 악성코드 감염이나 시스템에 대한 보안이 부족한 것으로 나타났다. 이러한 선박과 항만에서의 사이버보안 침해사고들은 선박충돌, 선박 운항 장애 및 정지, 인명피해, 금전적 피해 등의 피해를 입을 수 있어 보안대책마련이 필요하다.

해사 사이버보안 규정 및 지침은 국제기관과 우리나라의 한국선급을 포함한 각국의 선급별로 수립되어있다. 각 나라들의 선급에서 발표한 해사 사이버보안 지침은 국제기관들의 사이버보안 규정을 참조하고 있다. 그래서 국제 기준으로 볼 수 있는 IMO의 “Guidelines On Maritime Cyber Risk Management”와 BIMCO의 “Guidelines on Cyber Security Onboard Ships”, 그리고 한국 선급의 “해상 사이버보안 시스템 지침”을 비교하기 위해 우선적으로 한국 선급의 선박 등급에 따른 지침항목 중 중복되는 항목을 제외하고 통합하였다. 그리고 관리적 보안과 기술적 보안, 물리적 보안으로 분류하였다. 통합된 한국 선급의 사이버 보안 시스템 지침은 아래 [표 3-11]과 같이 관리적 보안에 해당하는 지침항목이 18개와 세부 지침 항목 74개, 기술적 항목에 해당하는 지침항목이 10개와 세부 지침항목 34개, 물리적 항목에 해당하는 지침항목이 3개와 세부 지침항목 20개로 통합되었다.

[표 3-11] 한국 선급의 사이버보안 시스템 지침(연구자 재구성, 2021)

구분	지침항목	세부 지침 개수
관리적 보안	보안체계의 일원화	1
	보안엔지니어링	1

	비즈니스 연속성 보장 및 강화	9
	사이버보안 시험	2
	사이버보안 심사	4
	사례 검토	1
	보안 정책	3
	보안 교육	4
	리스크 관리	6
	자산 관리	4
	침해사고 대응 및 복구, 역량 강화	17
	외부자 보안	3
	시스템 관리	9
	패치 관리	3
	모바일 보안	3
	소프트웨어 품질 관리	2
	변경 관리	2
기술적 보안	실시간 모니터링 역량 강화	3
	암호키 관리	1
	위협정보 수집체계 구축	1
	이상 징후 탐지	5
	데이터 보안	4
	로그 관리	5
	모바일 보안관리	1
	암호화	3
	악성코드 대응	1
	네트워크 관리	10
물리적 보안	접근 통제	7
	물리적 보안	11
	선박 내 물리적 통제 개선	2
합계		128

IMO의 사이버 위험 관리 규정과 BIMCO의 선박에 관한 사이버보안 지침, 한국 선급의 해상 사이버보안 시스템 지침을 비교한 결과는 아래 [표 3-12]와 같다. 비교한 결과로는 한국 선급의 지침이 IMO의 사이버 위험 관리 규정의 내용을 충실히 적용하고 있었다. 그러나 세부 지침 항목에 대한 모든 지침을 포함하지는 않는 것으로 분석되었다. IMO 규정의 세부 지침 항목에 대한 보완이 필요하다.

[표 3-12] 사이버보안 지침 비교(연구자 재구성, 2021)

한국선급 지침항목	IMO(NIST) 지침항목	BIMCO 지침항목
보안체계의 일원화	ID.GV	
보안엔지니어링	RS.AN	
비즈니스 연속성 보장 및 강화	ID.BE	
사이버보안 시험	RC.CO	
사이버보안 심사	RC.CO	Risk assessment
사례 검토	ID.RA, RS.CO, RS.AN	Identify Threats Respond to and recover from cybersecurity incidents
보안 정책	ID.GV, DE.DP	
보안 교육	PR.AT, RS.MI	
리스크 관리	ID,RM, RS.IM, RS.MI	Identify Threats Identify vulnerabilities Assessing the likelihood Risk assessment
자산 관리	ID.AM	Identify Threats Identify vulnerabilities Assessing the likelihood Impact assessment
침해사고 대응 및	ID.SC, PR.DS,	Develop protection

복구, 역량 강화	PR.PT, RS.RP , RS.CO, RS.AN, RS.IM, RC.RP, RC,IM, RS.MI	measures Develop detection measures Respond to and recover from cybersecurity incidents Establish contingency plans
외부자 보안	PR.AC, PR.AT	Identify vulnerabilities
시스템 관리	ID.AM	
패치 관리	PR.DS, PR.MA	
모바일 보안	ID.AM	
소프트웨어 품질 관리	ID.BE, ID,RM	
변경 관리	PR.IP, PR.MA	
실시간 모니터링 역량 강화	DE.AE, DE.CM	
암호키 관리	PR.DS	
위협정보 수집체계 구축		Identify Threats
이상 징후 탐지	DE.AE, DE.CM, DE.DP	Develop protection measures Develop detection measures
데이터 보안	PR.DS	
로그 관리	PR.PT	
모바일 보안관리	PR.AC	
암호화	PR.DS	
악성코드 대응	DE.CM	Develop detection measures
네트워크 관리	PR.PT	
접근 통제	PR.AC	
물리적 보안	PR.AC, PR.IP, PR.PT, DE.CM	
선박 내 물리적 통제 개선	PR.AC	

조선·해운산업분야의 사이버보안 침해사고 사례들의 유형과 원인 분석을 통해 관리적 보안 및 기술적 보안에 대한 개선방안이 필요함을 느낄 수 있었다. 우선 관리적 보안에 대한 개선방안으로는 조직 구성원의 보안인식 제고를 높여서 위기상황 시 대응능력을 강화시키는데 큰 도움이 될 것으로 판단한다. 이를 위해서는 보안전문가의 활동이 중요할 것이며 선장, 항해사, 승무원, 선원 등 非 IT담당자의 위기대응 능력을 높이는데 주력해야 할 것이다. 하지만 평소 사이버위협에 대해 인지가 부족한 상태이며 정기적인 보안교육을 받았다 하더라도 위기상황에 대처할 능력이 현저히 부족할 수밖에 없다. 기존에 이와 유사한 관리시스템들은 IT관리자만 운영하기 때문에 일반사람들은 e-mail 등으로 전파되는 랜섬웨어와 같은 사어비공격으로부터 대처가 부족할 수밖에 없다. 따라서 이러한 위기대응 능력을 이끌어줄 시스템화된 솔루션의 도움을 받는 것을 우선검토 할 필요가 있다.

한편, 기술적 보안에 대한 개선방안으로는 시스템의 잠재된 위협과 전산시스템의 부적절한 보안조치를 개선해야 할 것이다. 그리고 국내외 해양 사이버보안 규정 및 지침을 비교 분석한 결과로 우리나라의 해상 사이버보안 지침이 국제 규정에 맞추어 지침 개선이 필요한 부분을 보완해야 한다. 이러한 사이버보안 침해사고 사례를 통해 기존 사이버보안 지침의 문제점을 분석하고 개선사항을 도출하여 개선된 사이버보안 관리체계를 재정립하는데 다양한 노력을 해야 할 것이다.

제 4 장 조선·해운분야 사이버보안 모델 구현

제 1 절 사이버보안 모델 설계기준

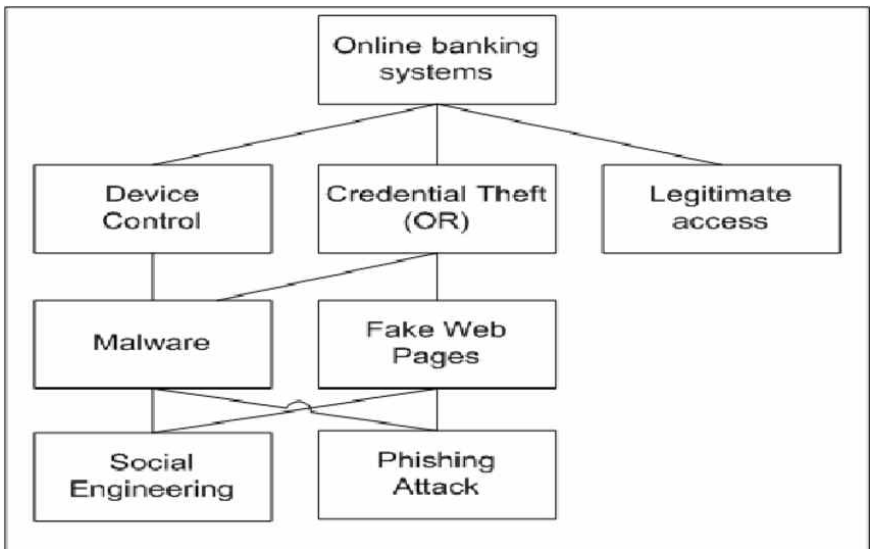
사이버보안 지침 및 IMO의 세부 지침 항목들의 비교분석을 통해 조선·해양분야에 적합한 사이버보안 관리체계의 재정립이 필요한 시기가 도래하였다. 해양안전 국제컨퍼런스 2017에서 스트래스클라이드 대학교 해양안전연구센터 바살로스 소장은 “200건이 넘는 해양사고에서 수백 명의 사상자가 생겼고 선박건조에 따르는 마진이 크게 줄고 해운의 경쟁은 치열해졌으며 관련 기술의 발전 속도가 빨라졌고 선박이 대형화됐다. 선박을 건조할 때부터 아키텍처에 안전을 고려한 설계가 이루어져야 한다.”고 주장하였다(구현모, 2017). 선박과 항만에 탑재되는 장비의 기술적 결함으로 발생가능하거나 내·외부의 사이버공격으로 인한 사고를 예방하기 위해 건조·건축의 설계단계에서부터 내재된 보안위협을 사전에 점검하고 보안위협을 차단하거나 피해를 줄일 수 있도록 도와줄 수 있을 것이라 판단해 볼 수 있다.

이에 본 연구에서는 사이버 보안위협 모델 구현을 위해 다음과 같은 요구사항을 도출하고자 한다. 우선, 사이버보안 규제를 이행하며 사이버보안 위협에 능동적인 대응을 위해서는 선박의 건조 단계에서부터 지침에 의거한 보안요구사항을 도출하여야 한다. 그리고 선박의 운항 단계에서는 기술적, 관리적, 물리적 분야별로 사이버 보안 체계를 정립하고 취약점을 도출하여 보완해야 한다. 이러한 보안 체계 정립을 통해 사이버 보안 위협 모델링을 설계하여 적용시키게 되면 위험평가 능력이 향상될 것이다. 위험평가는 위험관리의 일환으로 시행되며 정보보호관리체계의 인증과 주요정보통신기반시설 보안분석 및 평가 절차를 이행함에 있어서 중요 자산에 대한 피해를 사전에 예방할 수 있을 것이다.

사이버 보안을 위한 위협 모델링이란 위험분석을 하기 위해 잠재적인 위

협을 식별하고 분류하는 구조화된 방법이다. 즉, 위험(risk)을 추상화된 방법으로 표현하는 것이다. 시스템에 대한 이해부터 위협 식별, 위협 발생 가능성, 잠재적인 피해 및 영향, 위험에 기반한 완화책의 우선순위 및 계획을 포함한 일련의 과정으로서 조선·해운산업 분야에서의 사이버보안 위협 대응을 위한 최적의 방법론으로 효과적일 것이다(DSLAB컴퍼니, 2021).

위협 모델링은 위험분석을 위해 사용되며 웹서비스 및 인프라 등을 대상으로 모의해킹, 소스코드 진단 등 취약점 분석을 통한 보안진단을 통해 수집하고 있다. 위협분석 대상인 선박의 다양한 시스템, IoT디바이스, 기타 TCP/UDP 프로토콜 장비, 등을 분석할 수 있어야 한다. 아래 [그림 4-1]은 온라인과 연결된 시스템의 공격 루트를 구조화한 Attack Tree 의 예를 보여주고 있다.

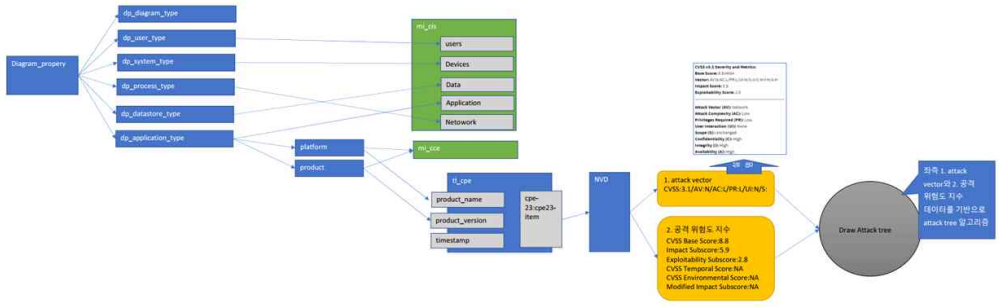


[그림 4-1] 온라인 시스템 Attack Tree 예시 (DSLAB컴퍼니, 2020)

제 2 절 사이버보안 모델 개발

조선·해운산업분야의 선박 및 항만을 건축·건조할 때 시스템 생명 주기의 설계단계에서 정보보호 관리체계를 구축할 수 있는 해사 사이버위협 모델링은 선박 및 항만에서 사용되는 IT와 OT 기술의 연결과 구성을 분석하여 내재된 보안위협을 도출할 수 있다. 우선 선박 및 항만의 설계자는 수요자의 요구에 맞추어 요구사항을 분석하게 되고 요구사항에 따라 설계 작업을 진행하게 된다.

설계 작업에는 크게 상류 설계와 하류 설계로 구분할 수 있으며 상류 설계는 선박 사양을 비롯한 선주의 요구사항과 국제 협약을 포함한 규정 및 규칙을 만족하는 선박의 성능 설계 과정으로 보통 개념 설계부터 상세 설계의 일부를 포함하고 있다고 정의할 수 있다. 하류 설계는 상세 설계 후반부터 생산 설계까지 포함하며 적기에 생산 정보를 생성하기 위한 설계 과정으로 정의할 수 있다.(쿠니히로, 2013; 이정렬 外, 2017)



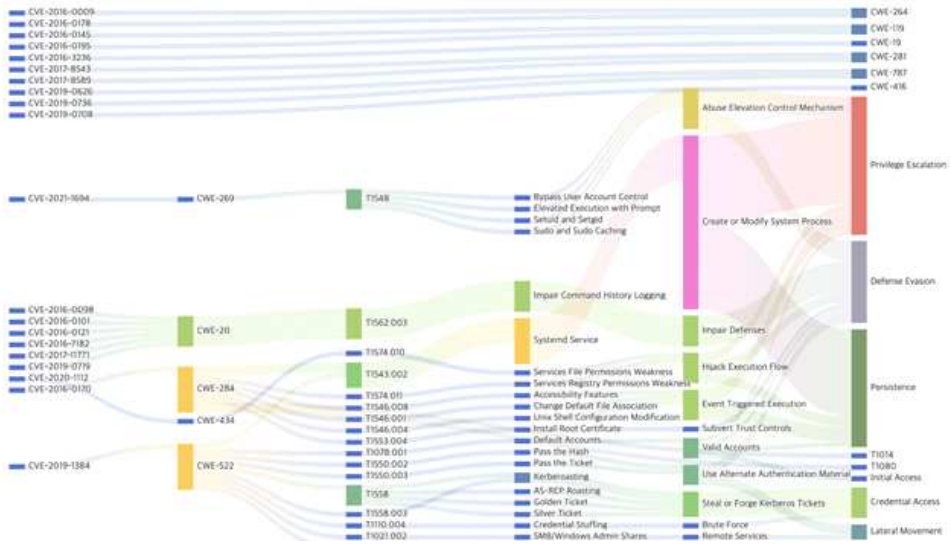
[그림 4-2] 선박 사이버위협 모델링(DSLAB컴퍼니, 2021)

설계단계에서 선박의 룸(Room)이나 항만의 구역별로 데이터 흐름도(Data Flow Diagram)의 하드웨어 또는 소프트웨어, 장비, 사용자, 행위자, 통신방식, 프로토콜 등과 같은 구성요소를 배치하고 구성요소 간의 데이터 통신 연결 관계를 연결하며 구성요소의 속성들을 설정한다. 각각의 구성요소 또는 구성요소 간의 관계를 위협정보 데이터베이스에서 검색한다. 위협정보 데이터베이스인 Attack Library는 데이터 흐름도를 작성한 이 후 시스템에 대한 위협

들을 사고사례, 기술보고서, 논문, 컨퍼런스 및 CVE(Common Vulnerabilities and Exposure)의 다양한 자료 조사를 통해 수집한 목록으로 구성되어있다(조용현, 2019). 검색된 위협정보를 이용하여 Attack tree를 구성하고 공격 경로를 지정하여 위협정보가 최종적으로 선박 또는 항만에 미치고자 하는 목표를 도출한다. 이러한 과정의 사이버 위협 모델링 아키텍처 모형은 위 [그림 4-2]와 같이 나타낼 수 있고 DFD구성요소의 내재된 보안위협을 판별 할 수 있다.

제 3 절 사이버보안 모델 구현

구성요소들을 데이터 흐름도에 배치 및 연결, 설정하고 내재된 보안위협을 분석하여 도출된 보안위협은 구성요소 단일객체 또는 연관객체 사이에서 상호 영향을 끼칠 수 있는 위협이다. 이러한 내재된 보안위협들은 시스템 장악, 시스템 마비, 장애 발생 등을 최종적인 목표를 가지게 된다.



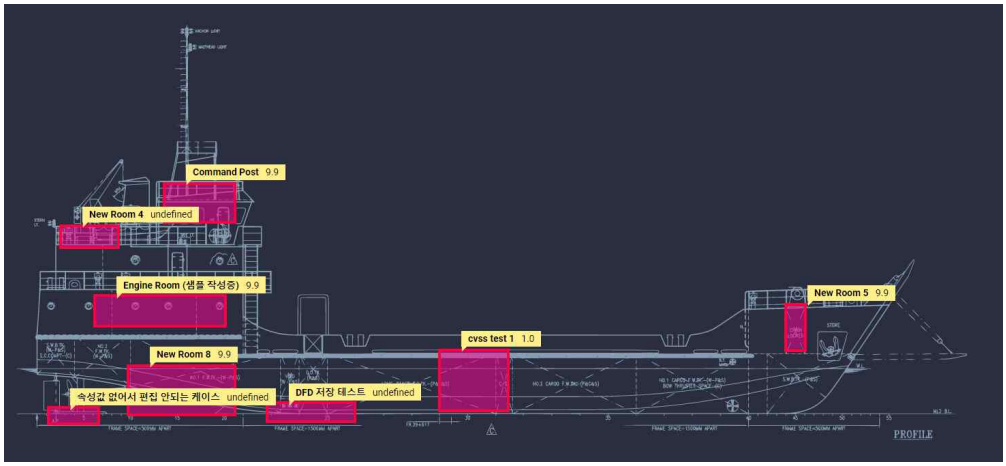
[그림 4-3] 사이버 공격 경로 Flow Chart(DSLAB컴퍼니, 2021)

구성요소에 내재된 보안위협을 Attack List기반으로 분석하고 위협정보 데

이터베이스 Attack Library에서 식별하여 Attack Tree를 작성한다. Attack Tree의 최종 경로가 구성요소의 잠재적 위협의 최종 목표가 될 수 있으며 [그림 4-3]는 각각의 보안위협이 최종적으로 공격목적까지의 경로들을 나타낸다.

분석을 통해 식별된 잠재적 사이버위협은 공통 취약점 등급 시스템(CVSS, Common Vulnerability Scoring System)을 이용하여 선박의 룸이나 항만의 구역별로 보안 취약성에 대해 정량화한 수치로 표시할 수 있었다. CVSS는 정량화된 수치에 따라 저위험군은 0.1점부터 3.9점까지, 중위험군은 4.0점부터 6.9점까지, 고위험군은 7.0점부터 8.9점까지, 치명적 위험군은 9.0부터 10.0점까지 네 가지로 분류할 수 있다.

[그림 4-4]과 같이 사이버보안 위협 모델링을 통해 선박 또는 항만의 각 구역에 설계된 구성요소들의 내재된 보안위협의 점수를 산출하고 이를 선원 또는 관리자에게 알려줌으로서 보안위협에 대한 경각심을 파악하고 보안설계를 할 수 있었다.



[그림 4-4] 선박의 각 룸의 구성요소에 따른 보안위협(DSLAB컴퍼니, 2021)

잠재적 보안 위협과 공격경로, CVSS를 통한 정량화 수치를 통해 조선·항만 관련 실무자들에게 설계단계에서 사이버보안 취약성의 경각심을 일깨울 수 있을 것으로 기대되며 식별된 잠재적 보안 위협에 대한 해결방안을 제시

함으로써 안전한 선박과 항만의 건축·건조에 기여할 수 있을 것이다.

본 연구를 통해 보안위협은 정량화 수치로 표현할 수 있었으며 이를 구역별로 취합된 결과로 나타낼 수 있었다. 보안위협이 실제 공격의 최종 목적으로의 공격경로를 식별이 가능하였으며 보안위협이 최종 공격 목적으로 연결되는 것을 조선·항만 관련 실무자들에게 보안위협을 인지시키고 보안위협을 사전에 예방할 수 있을 것으로 기대한다.

한편, 조선·해운산업분야에서 발생한 사이버보안 침해사고 사례의 원인과 유형에 대한 분석에서 인적 보안 사고를 방지하기 위한 관리적 개선방안으로 정보보안 교육을 강화하여 보안인식을 향상시키기 방법이 도입되고 있다. 아래 [그림 4-5]는 메타버스를 활용한 사이버 보안모델 체험의 예로서 非IT 인력도 사이버침해 위협에 대해 능동적으로 대처가 가능하도록 훈련이 용이한 시스템으로서 좋은 평가를 받고 있다.

[그림 4-5] 메타버스를 이용한 훈련(MarineLink; 김진, 2021)

이를 위해 관련 종사자에 대한 정보보안 교육 및 훈련이 요구되는 실정이다. AR, VR, 메타버스 기술을 활용한 3차원적 사용자 경험을 교육과 접목하여 큰 효과를 기대할 수 있다. 첫 번째, 온라인 교육 및 세미나를 활용하여 오프라인 교육의 한계를 초월할 수 있다. 두 번째, 가상 선박의 구현을 통해

사이버보안의 위험 요소를 학습할 수 있다. 세 번째, 선박 시스템의 모의해킹 학습과 사고를 재현하고 파급효과를 체험할 수 있으며, 네 번째, 조선 해양 사이버보안을 위한 전시관을 운영하여 사회적 인식 강화 및 안보 의식을 고취할 수 있다(김진, 2021).

제 5 장 결론

제 1 절 결론 및 시사점

본 논문은 조선·해운산업에서 ICT와 OT가 융합되는 선박 및 항만을 건조·건축·운영하는데 있어서 사이버위협에 대한 인식제고를 높이고 정보보안 관리체계의 수준을 향상시키기 위해 국제기구의 사이버보안 지침 및 가이드라인을 분석하였다. 그리고 국·내외 선급에서 기준하고 있는 보안지침을 비교분석하여 우리나라 선박·항만에 적합한 사이버보안 모델을 구현하는데 목적을 두고 있다.

우선 조선·해운산업분야에서 발생한 사이버보안 침해사고 사례 분석을 통해 관리적, 기술적, 물리적 보안 인식제고를 위한 가이드라인을 제시하였으며 좀 더 체계적이며 자율적 참여를 유도하기 위해서 AR, VR 기술기반의 메타버스 플랫폼을 활용한 사이버보안 모델 체험 및 훈련방안을 제시하였다.

그리고 해사 사이버보안 지침들의 비교분석과 선박 및 항만에 탑재된 장비의 내재된 보안위협을 예방하기 위해서 설계단계에서의 보안위협을 식별하기 위한 사이버보안 관리체계를 아키텍처를 연구하였다. 내재된 보안위협의 식별과 최종적인 공격목표에 도달되는 과정을 공격경로로 표시, 보안위협에 대한 정량화된 수치를 통해 조선·항만 관련 실무자들에게 보안위협을 인지시킬 수 있고 식별된 보안위협에 대한 해결방안을 제시함으로써 조선 산업과 해운산업에 안전한 사이버환경을 조성할 수 있을 것이다.

본 연구를 통해 조선·해운산업분야에서 발생할 수 있는 사이버보안 침해사고를 예방하고 보안위협 요소를 감소시킬 수 있는 실무적인 사이버보안 관리체계를 강화할 수 있었다. 그리고 조선·해운산업분야에서 가장 중요시 하는 프로세스인 운항 및 운영관리에 있어서 서비스 지속성과 운영관리의 효율성을 향상시킬 수 있을 것으로 기대한다. 이를 통해 우리나라의 조선 산업과 해운산업이 글로벌 경쟁력을 유지하고 국가위상제고에 지속적으로 기여할 것으로 기대한다.

제 2 절 연구의 한계점 및 향후 연구방향

본 연구는 국제기구를 포함한 국내외 선급의 사이버보안 지침 및 가이드라인을 비교 분석하여 우리나라 선급의 기준을 충족하는 개선된 보안체계와 사이버보안 모델을 구현 했다는 점에서 연구의 의의가 있다고 할 수 있다. 그러나 우리나라 선급 기준으로 제한하였기에 국외 조선·해양산업분야에는 당장 적용이 어려울 수 있다는 한계점이 있다. 그리고 선박위주의 사이버보안 모델 구현 방안으로 조선·해양산업분야의 항만과 해양플랜트 등에서의 특수성을 적용하기에는 다소 시행착오가 있을 수 있다. 향후 연구를 보완한다면 선박뿐만이 아니라 항만과 해양플랜트에도 사이버 보안 모델의 적용이 가능할 수 있을 것이다. 하지만 우리나라가 조선·해양산업분야 에서는 글로벌 경쟁력 수준이 최상위권을 유지하고 있는 만큼 향후 연구로서 국제기구 및 글로벌 선급의 기준을 충족하는 보안관리체계를 수립하고 사이버보안 모델을 구현, 적용시킨다면 나아가 글로벌 해상 사이버안전지대의 파수꾼 역할을 할 수 있을 것으로 기대한다.

참 고 문 헌

1. 국내문헌

양해성, 곽기호, 전유수.(2021).한국 조선 산업의 주도권 회복에 대한 탐색적 연구: 최근 고부가가치 선종 수주 성과를 중심으로.한국혁신학회지,16(1),121-158.

장정재. (2020). 중국 조선기자재 산업의 부상과 한국기업의 대응방안. 한중관계연구, 6(2), 57－80.

김진근. (2008). 경남의 4대 전략산업 현장의 목소리. 정책포커스 이슈분석.1-43. p.3.

한국조선해양기자재연구원. (2016). “조선업 선종별 Lifecycle 분석 및 조선기자재업 동 반 성장 전략 연구: 중형조선소 분석을 기반으로”.

홍성인. (2017). “조선 해양 산업의 발전기반 분석과 재도약 전략”. 산업연구원.

이경묵, 박승엽 (2013). 『한국 조선 산업의 성공요인』, 서울대학교 출판문화원.

양종서, 임종수 (2019). “조선업 전망 및 향후 발전 전략” 『한국은행 경남본부』.

곽기호. (2019). 우리나라 중공업 정책의 창건자. 한국과학기술연구원. 기술혁신연구. 27(5), 155－187.

양종서, 김창록. (2016). “한중일 조선업 경쟁력 분석 및 전남 중형 조선 산업 지속 발전 전략”. 『한국은행 목포본부』.

이경래. (2018). “선박 금융시장에서 중국금융 리싱의 부상과 시사점”. 『무역보험연구』. 19(1).

이은창, 남상욱, 양종서, 홍성인 (2019), “한국 조선산업의 중장기 전망과 정

책과제,”『산업연구원』. 정책과 제, 2019-915.

남은영, Li Kai, Wang Yi. (2020). China’s Shipbuilding Industry: Perspectives on Windows of Opportunity. 현대중국연구, 22(1), 133－174.

장세진. (2019).『글로벌경영』. 박영사.

하나금융투자. (2020). “조선/기계 - 바이든 시대, 10년간에 걸친 친환경 선박 교체기 도래,”.『하나금융투자 Today’s Talk』

안영균. 김보람. (2021). 해운산업의 스마트화를 선도할 기술개발 수요조사 연구. 국제상학, 36(1), 105－127.

이석호. (2009). 우리나라 해운·항만산업 활성화를 위한 인프라 확충 방안.

박영태, 류광열, 김동윤. (2020). “4차 산업혁명시대 부산신항 배후단지 뉴비즈니스 모델 도출을 위한 전략 과제”, 「국제상학」, 제35권 제2호, 한국국제상학회.

최두원. (2020). 스마트 물류 구현을 위한 핵심기술과 적용동향에 관한 연구. 국제상학, 35(4), 135－157.

이우영. (2020).『LNG 선박연료 판매량 3배 급증』. 조선비스. 2020.05.20.

박한선, 박혜리, 유윤자, 박상원 (2019). 해상 사이버 보안체계 강화방안 연구. 연구보고서, 1-231.

이은수. (2021). 선박 사이버보안 강화를 위한 법제 개선방안에 관한 연구. 석사학위논문

이은수, 박성호. (2021). 선박 사이버보안 강화를 위한 입법론적 연구. 海事法硏究, 33(2), 227－254

최건우, 윤재웅, 나정호. (2020). 컨테이너 해운-조선산업 관계분석 연구

안영균, 김보람. (2021). 해운산업의 스마트화를 선도할 기술개발 수요조사 연구. 국제상학, 36(1), 105－127.

이재성, 박세훈. (2021). 최근 글로벌 해운 환경 변화와 국내 대응 방안에 관

한 연구. 해양비즈니스, 49(1), 99－122.

조성대. (2021). 최근 해상운임 상승 원인과 중소기업 물류비 절감 방안. 트레이드 포커스. 2021년 15호. 한국무역협회 국제통상연구원.

김경석. (2021). 디지털사회를 대비한 일본의 법률정비와 의미 - 디지털사회형성기본법을 중심으로 -. 국제법무 / International Law Review, 13(2), 1.

박종승. (2019). 스마트워크 환경에서의 ISMS-P 기반 정보보호 감리 모형 연구. 석사학위논문.

선종욱, 이경호. (2021). Dea 모형을 이용한 주요정보통신기반시설 취약점 분석·평가의 효율성 분석. 정보보호학회논문지, 31(4), 853－862.

식품의약품안전처 식품의약품 안전평가원, (2017). 『의료기기의 사이버 보안 허가·심사 가이드라인(안) (민원인 안내서)』. 의료기기심사부 첨단의료기기과.

김금현. (2019). 의료기기 사이버 보안 규제에 대한 대응방안. 석사학위논문.

이홍걸. (2007). 컨테이너 터미널의 정보보호 수준 제고를 위한 통합 평가지수 개발에 관한 연구. 해운물류연구.

한국선급. (2021).『해상 사이버보안 시스템 지침, 2021.』

Panam Choi, & Seungwhoon Han. (2015). 직위에 따른 기업정보보호활동 인식이 산업기밀유출에 미치는 영향. 한국재난정보학회논문집, 11(4), 475－486.

김진 (Jin Kim). (2021). 메타버스를 활용한 조선 해양 분야 정보보호 교육 콘텐츠 개발 방안. 정보보호학회논문지, 31(5), 1011－1020.

백영균. (2010).『가상현실공간에서의 교수-학습』. 서울: 학지사.

손지영. (2018). 장애학생 교육에 가상현실 기술을 적용한 국내 중재연구의 분석. 특수교육 저널 : 이론과 실천, 19(1), 233.

박현린, 손은남. (2020). 가상현실 및 증강현실 기술을 기반으로 한 매체의

교육적 효과에 대한 국내 동향 연구. 학습자중심교과교육연구, 20(5), 725－741.

김성덕, 이용국. (2021). 해양안전 가상현실 체험교육의 효과성에 관한 연구. 디지털융복합연구, 19(3), 437-444.

계보경. (2007). 증강현실(Augmented Reality) 기반 학습에서 매체특성, 현존감(Presence), 학습몰입(Flow), 학습효과의 관계 규명. 박사학위논문.

남선혜, 이정민. (2020). 국내 증강현실활용교육의 효과에 대한 메타분석. 교육정보미디어연구, 26(1), 129-156.

이기성, 정유선, 정유선, 임태형, 류지헌. (2021). 메타버스를 활용한 대학생 온라인 수업에서 공간이동 수준이 학습실재감과 흥미발달에 미치는 효과. 교육정보미디어연구, 27(3), 1167-1188.

홍희경. (2021). 메타버스의 교육적 적용을 위한 탐색적 연구. 문화와 융합, 43(9), 1－22.

구현모. (2017). 최신 해양안전 이슈 망라하다 : “안전과 위험이 선박설계 단계부터 고려되어야” 6월 14일, 15일 부산 벡스코 컨벤션홀 1층 안전 분야 전문가 200여명 참석. 해양한국 / Maritime Korea, 2017(7), 98.

이정렬, 박호균, 손명조.(2017).선박설계의 새로운 패러다임.대한조선학회지,54(1),3-6.

조용현, 차영균. (2019). 위협 모델링을 이용한 선박 사이버보안 요구사항 연구. 정보보호학회논문지, 29(3), 657－673.

DSLAB컴퍼니. (2020). 조선·해양산업분야의 사이버보안 위협대응 가이드라인 v 1.0

DSLAB컴퍼니. (2021). 조선·해양산업분야의 사이버보안 위협대응 가이드라인 v 2.0

2. 국외문헌

Robert Hassink, & Dong-Ho Shin. (2005). South Korea's Shipbuilding Industry:From a Couple of Cathedrals in the Desert to an Innovative Cluster. 기술혁신연구, 13(2), 133-156.

Manuel E. Sosa, Steven D. Eppinger, & Craig M. Rowles. (2004). The Misalignment of Product Architecture and Organizational Structure in Complex Product Development. Management Science, 50(12), 1674-1689.

Kiamehr, M., Hobday, M., & Kermanshah, A. (2014). Latecomer systems integration capability in complex capital goods: the case of Iran's electricity generation systems. Industrial & Corporate Change, 23(3), 689-716.

Ruuska, I., Ahola, T., Martinsuo, M., & Westerholm, T. (2013). Supplier capabilities in large shipbuilding projects. International Journal of Project Management, 31(4), 542-553.

Lim, C., Kim, Y., Lee, K.. Changes in industrial leadership and catch-up by latecomers in shipbuilding industry†. Asian Journal of Technology Innovation, 25(1), 61-78.

Vishnevskiy, K., Karasev, O., Meissner, D., Razheva, A., & Klubova, M. (2017). Technology foresight in asset intensive industries: The case of Russian shipbuilding. TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE, 119, 194-204.

Martin Stopford. (2020). "Coronavirus, Climate Change & Smart Shipping THREE MARITIME SCENARIOS, 2020-2050".

Azuma, R. T. (1997). A survey of augmented reality. PRESENCE:

Teleoperators & Virtual Environments, 6(4), 355.

BIMCO. (2020). Safety at Sea and BIMCO cyber security white paper.

ClassNK. (2019). ClassNK Cyber Security Approach.

BIMCO. (2020). Guidelines on Cyber Security Onboard Ships V4.

NIST. (2018). NIST_2018-04-16_framework v1.1.

IMO. (2017). MSC-FAL.1-Circ.3 - Guidelines On Maritime Cyber Risk Management (Secretariat).

DNV. (2021). CG-cyber secure, 2021.

BV. (2020). Rules on Cyber Security for the Classifi cation of Marine Units.

ABS. (2021). A PRIMER ON IMO CYBER RISK MANAGEMENT GUIDELINES.

MarineLink, "Maritime Simulation & Training : a partnership that pays off", https://www.marinelink.com/news/maritime-simulation-training -a-468007, Nov 20, 2021.

ABSTRACT

Analysis of shipbuilding and shipping industry security management system and research on cybersecurity model implementation plan

Choi, Oong-Jae

Major in Educational Administration

Dept. of Educational Administration

The Graduate School

Hansung University

Korea is facing a future convergence society after the 4th industrial revolution and is in a time when it is necessary to respond to the rapid change of the smart convergence industry. The convergence of ICT and OT in the shipbuilding and shipping industry, which maintains the world's highest level, is transforming digitalization and automation as a whole. Recently, as the demand for autonomously operated ships, smart ships, and smart ports has increased, cyber threats to ships and ports have increased. As the 『Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.』 was amended in December 2020, the convergence ICT sector was also subject to information protection regulations, and ships were added to the transport sector as information and communications network connection

devices. The need for is further emphasized.

As the number of connections to the Internet increases due to the automation and digitalization of ships and accessories, cybersecurity threats have increased. The Internet connection for convenience caused damage to the point that ships were stopped due to hacking and malicious code infection, which caused great property damage. In June 2017, Denmark's largest shipping company, A.P. As Moller - Maersk was attacked by ransomware, an astronomical amount of financial damage of over 300 billion won was issued. In addition, cyber security breaches continue to occur in domestic and foreign shipbuilders and shipping companies, ships and ports.

Accordingly, the International Maritime Organization has suffered material damage due to damage or loss of important information or systems due to maritime cyber threats, or property damage caused by system disruption in transportation and operation. As the anxiety caused by such cyber threats is rapidly increasing, the recent announcement of 'Cyber Risk Management' in January 2021 and emphasizing compliance has been made.

Through the results of this study, it is expected that it will serve as an opportunity to recognize and improve cybersecurity problems that may occur in the shipbuilding and shipping industries. For this study, cybersecurity guidelines and guidelines based on international maritime organizations and domestic and foreign shipping levels were analyzed, and cybersecurity modules were implemented to solve the problems found, and finally, an improved management system was suggested.

It is expected to contribute to improving cybersecurity levels and preventing security threats in the shipbuilding and shipping industries in the future. In addition, as Korea's shipbuilding and shipping industries maintain the highest level of global competitiveness, it will be possible to

establish a security management system that meets the standards of international organizations and global advancement by conducting additional research activities in the future. Therefore, by presenting a leading security management system model, Korea will be able to provide an opportunity to serve as a watchman in the global maritime cyber safety zone.

【Keyword】 Ship cybersecurity model, Cyber Risk Management, Maritime cyber breach, Maritime cybersecurity, Cybersecurity awareness