Journal of the Korean Society of Marine Environment & Safety
Research Paper
Vol. 28, No. 7, pp. 1140-1147, December 31, 2022, ISSN 1229-3431(Print) / ISSN 2287-3341(Online) https://doi.org/10.7837/kosomes.2022.28.7.1140

IPA분석을 활용한 해상교통관제 인원의 사이버 보안 관리 인식 연구

박상원* · 정민지* · 유윤재**† · 윤경국***
* 한국해양수산개발원 물류·해사산업연구본부 연구원, ** 한국해양대학교 항해융합학부 교수,
*** 한국해양대학교 해사인공지능·보안학부 교수

A Study on Cyber Security Management Awareness of Vessel Traffic Service Personnel Using IPA

Sangwon Park* · Min-Ji Jeong* · Yunja Yoo**† · Kyoung-Kuk Yoon***
* Researcher, Division of Logistics and Maritime Industry Research, Korea Maritime Institute, Busan 49111, Korea
** Professor, Division of Navigation Convergence Studies, Korea Maritime & Ocean University, Busan 49112, Korea
*** Professor, Division of Maritime AI & Cyber Security, Korea Maritime & Ocean University, Busan 49112, Korea

요 약 : 디지털 기술의 발전에 따라 해상환경은 빠르게 변화할 것으로 예상된다. 자율운항선박의 경우 국내·외 많은 국가에서 기술개발 중이며, 국제사회는 이를 운용하기 위한 논의도 시작되었다. 선박의 변화는 해상교통 환경의 변화를 야기하며, 육상지원시설에 대한 변화도 촉구한다. 본 연구는 항행지원시설의 사이버 보안 체계 개선을 위해 해상교통관제 인원의 사이버 보안 관리 인식을 분석하고자 한다. 이를 위해 해상교통관제 중심으로 사이버 보안 관리 현황을 살펴보고, 해상통관제 인원을 대상으로 설문조사를 실시하였다. 설문조사 분석은 IPA 방법론을 활용했으며, 분석결과 보안담당 경험이 있는 인원과 경험 없는 인원의 사이버 보안에 대한 인식차이가 뚜렷하게 나타났다. 더불어 사이버 공격 탐지 및 차단 관련 기술적인 조치가 가장 우선적으로 시행되어야할 사항으로 나타났다. 본 연구 결과는 항행지원시설에 대한 사이버 보안 관리 체계 개선을 위한 기초자료로 사용될 수 있다.

핵심용어 : 사이버 보안, 해상교통관제, IPA 분석, 자율운항선박, 항행지원시설

Abstract : *With the development of digital technology, the marine environment is expected to change rapidly. In the case of autonomous vessels, technology is being developed in many countries, and the international community has begun to discuss ways to operate it. Changes in ships cause changes in the marine traffic environment and urge changes to aids to navigation. This study aims to analyze the cyber security management awareness of VTS personnel to improve the cyber security system for aids to navigation. To this end, the current status of cyber security management was reviewed with a focus on VTS, and a survey was conducted on VTS personnel. The survey analysis used the IPA methodology, and as a result of the analysis, a clear difference was observed in the perception of cybersecurity between those with experience in security and those without experience. In addition, technical measures related to cyber-attack detection and blocking should be implemented with the highest priority. The results of this study can be used as basic data for improving the cyber security management system for aids to navigation.*

Key Words : *Cyber security, Vessel Traffic Service, IPA, MASS, Aids to Navigation*

1. 서 론

국제해사기구(IMO)에서 자율운항선박 논의가 본격화 되면서, 조선 업계의 기술개발도 활발히 이루어지고 있다. 그러나 선박 분야의 사물인터넷, 빅데이터, 인공지능 등 4차 산업혁명 기술 도입의 이면에는 사이버 보안 위협이 있다. 지난 2017년의 머스크사의 랜섬웨어 공격이나 같은 해 해적의 해킹에 의한 독일 컨테이너선박의 항해시스템 중단 사고는 사이버위협의 위험성을 알 수 있는 사례이다(Asiaeconomy, 2022). 이에 따라 국제기구도 사이버 보안 지침을 발표하고 있다. 국제해사기구는 해상사이버 리스크 관리에 관한 결의서를 채택하고, 사이버 보안을 관리토록 권고하고 있으며, 국제항로표지협회는 항행지원시설에 대한 사이버 보안을

* First Author : psw6745@kmi.re.kr, 051-797-4919
† Corresponding Author : yjyoo@kmou.ac.kr, 051-410-4286

논의하고 있다(IMO, 2017; IALA, 2021). 선주협회에서도 안전관리적합증서 심사에 대비하기 위한 선박 사이버 보안 가이드라인을 제공하고 있다(BIMCO, 2020). 최근 국제선급협회는 신조선과 선박에 탑재되는 기자재 시스템 사이버 보안 통합 요구사항을 수립했으며, 2024년 1월 이후 건조 계약을 체결한 신조선부터 강제 적용될 예정이다(IACS, 2022a; IACS, 2022b).

선박 기자재의 디지털화는 선박과 선박 간 통신 뿐만아니라 육상 간 통신도 영향을 미친다. 그러므로 육상시설과 선박 간의 사이버 보안 관리도 필요하다. 본 연구에서는 대표적인 항행지원시설인 해상교통관제(VTS, Vessel Traffic Service)를 중심으로 사이버 보안 관리 현황 및 사이버 보안 취약성을 개선하기 위한 방안을 살펴보고자 한다. 이를 위해 관련 선행연구 분석을 통해 본 논문의 차별성을 제시하고, 사이버 보안 관리 사례를 조사하였다. 이를 바탕으로 사이버 보안 취약성 개선을 위한 설문조사를 VTS 인원 대상으로 수행했다. 설문조사 분석은 중요도-성취도 분석 방법론을 활용했으며, 결과를 바탕으로 해상교통관제 측면에서 사이버 보안 관리를 위해 집중적으로 개선해야하는 요소를 도출하고자 한다.

2. 선행연구 분석

D'agostini and Jo(2019)는 선원을 대상으로 보안교육과 선원 보안인식 및 선박의 보안성 사이의 관계를 분석하였다. 분석 결과 선박 보안교육을 이수한 선원은 선박 보안에 대한 인식이 높고, 보안인식이 높으면 선박의 보안에 긍정적인 영향을 미치는 것을 확인하였다. 즉 보안교육은 선원의 보안인식과 보안성과에 중요한 역할을 미치기 때문에 해당 교육의 당위성을 증명했다고 볼 수 있다. Yoo et al.(2018)은 국가 주요 기반 시설로서의 VTS 시스템의 정보 보안의 현황을 분석하고 앞으로 개선해야 할 점을 관리적, 물리적, 기술적 측면에서 살펴보았다. 관리적 측면에서는 VTS 시스템을 운영하는 관제사 뿐만 아니라 센터장의 보안 필수 교육을 위한 프로그램의 개발 및 운영이 필요하다고 했다. 물리적 측면에서는 통합 보안 관제센터의 신설이 필요함을 주장했다. 기술적 측면에서는 로그 서버와 무선 침입차단 시스템 구축을 통해 보안 강화 방안이 필요함을 주장했다. Park et al.(2020) 자율운항선박 도입에 따른 해상교통관제 체계 개선방안을 제안하였다. 특히 자율운항선박이 양방향 통신 인프라를 기반으로 하는 디지털 센서의 집합체임을 고려하여 원격운항센터가 관제 범위에 추가되는 경우 이에 따른 사이버 보안 이슈가 더욱 중요해지고 이에 따라 고려해야 할 사항을 관리적, 기술적, 물리적 측면에서 검토했다. 관리적 측면에서는 해상 사이버 보안을 관리하기 위한 국내법 도입, 기술적 측면에서는 정보관리체계 도입, 물리적 측면에서는 원격운항센터를 포함한 VTS 관리 영역 확대를 제시하였다. Kim(2022)는 자율운항선박 등장에 따른 선박교통관제사 교육 훈련 체계 개선방안을 제안하였다. 개선방안은 자율운항선박에 대한 이해, 사이버 보안, 의사소통방안, 비상상황대응 측면에서 제시하였다. 특히 사이버 보안은 자율운항선박의 특성을 고려해 장비, 정보, 시설에 대한 보안시스템 및 인증체계에 대한 교육 강화가 필요하다고 주장했다. Lee et al.(2020)은 선박의 디지털화와 더불어 다가오는 사이버 보안 사고 위협에 대응하고자 선박 사이버 보안 책임자 교육 과정안을 제시하였다. 제안한 교육은 총 16시간 과정이며, 사이버 보안 관련 국내외 동향, 규정, 사이버 보안 평가, 사이버 보안 계획서, 선박 사이버 보안 관리 시스템구축 절차 및 방법 등으로 구성되어 있다. 그리고 이에 따라 선원법, 선박직원법 및 국제항해선박 및 항만시설의 보안에 관한 법률 개정 필요성을 주장했다. Chang and Kang(2012)는 항만기업 종사자들의 정보 보안인식 정도와 지각된 정보 보안위험 정도에 영향을 미치는 요인들을 구조방정식을 활용하여 도출하고자 했다. 분석결과 정보 보안 교육은 정보 보안인식에 영향이 있었으며, 위협, 취약성은 지각된 정보 보안위험에 유의한 영향을 미치는 것으로 나타났다. 항만기업 종사자 대상의 실증분석으로 다른 분야까지 동일한 결론을 내릴 수는 없지만, 정보 보안에 관한 교육은 인식에 영향이 있다는 보편적인 결론을 도출할 수 있었다. D'agostini et al.(2017)은 무인화 선박에 대한 한국 선원의 지식과 인식에 대한 연구를 수행했다. 선원은 가까운 미래에 무인선은 등장하기 어려울 것이라는 인식이 강하며, 물리적 결함과 수리에 대한 취약성을 단점으로 제시하였다. 아울러 선박자동화는 해킹이나 보안 취약성도 문제가 될 수 있는 등 부정적인 인식이 강했다. 한편 일자리 측면에서는 무인선 등장으로 일자리 축소는 크게 인식하지 못하며, 선원고용보다는 선박 안전성 확보에 대한 인식이 강한 것으로 나타났다. Kim and Yang (2019)은 자율운항선박 개발 및 운용과정에서 고려해야 할 주요 인적요소 이슈를 고찰하고 육상센터의 제어에 따라 예상되는 육상운항사의 의사결정 및 업무수행에 영향을 미치는 요소에 대한 평가를 수행했다. 특히 VTS 관제사의 변화에 대해 제시했으며, 자율운항선박, 육상운영자 및 유인선박, VTS 관제사 간 통신에 대한 가용성, 신뢰성 및 보안을 담보할 수 있는 시스템이 필요하다고 주장했다. 그리고 자율운항선박은 사고에 대한 인적요인을 줄일 수 있으나, 인적요인에 대한 위험성은 육상운영자나 시스템 개발자로 이동하는 것이라 했다. 즉 자율운항선박 개발에 있어 다양한 인적 요인을 고려 할 필요가 있다고 하였다. Lim(2022)은 사

이버 보안 관련 국제사회의 동향을 분석하고 해상 사이버 회복 탄력성 확보를 위해 해상 사이버 보안 관리체계 구축, 설계보안 및 해상 사이버 보안 전문 인력 양성에 대한 제언을 했다. KMI(2019)는 국내외 해상 사이버 보안 관리 실태 및 취약성을 분석하고 주요국의 사이버 보안 관련법 제도 및 정책을 종합적으로 고려해서 해상분야 사이버 보안 취약성 개선을 위한 방안을 제안했다. 취약성 개선 요소 우선순위를 AHP를 활용하여 도출했으며, 기술적 보안이 36.3%, 관리적 보안이 35.6%, 물리적 보안이 28.1%의 중요도를 가지는 것으로 나타났다.

본 연구는 VTS에서 실무를 담당하는 인력을 바탕으로 설문조사를 통해 현재 VTS의 사이버 보안에 대한 현황을 분석하고, 취약성 개선을 위해 Importance-Performance Analysis(이하, IPA) 방법론을 활용하여 제언하고자 한다. 기존연구와 비교하여 VTS 인원에 한정하여 사이버 보안 인식을 조사한 것에 차별성이 있다. 이는 해사안전 광의의 영역이 아닌 해상교통관제 측면에 집중하여 사이버보안 실태 및 개선방안을 볼 수 있다는 점에서 의의가 있다. 또한 선행연구의 AHP 방법론은 중요도 등 하나의 요인에 대한 쌍대비교로 우선순위를 결정하는 반면, IPA 방법론은 중요도와 만족도의 두 가지 요인을 동시에 고려하여 정책방향을 결정할 수 있는 방법이다. 본 연구는 연구대상 범위 및 방법론에서 기존 선행연구와 차별성이 있다.

3. 해상 사이버 보안 대응 현황

3.1 해상 사이버 보안 사고 사례

2017년 6월 머스크라인의 17개소의 항만 터미널 IT 시스템이 랜섬웨어 공격을 받았으며, 그 결과 컨테이너 선적작업은 3주간 수동으로 전환되었다. 총 피해 규모는 3,000억으로 추산되며, 서버 4,000대, PC 45,000대, 소프트웨어 2,500개가 재설치된 바 있다. 특히 공격에 사용된 NotPetya 랜섬웨어는 암호화된 데이터를 복구하는 것이 원칙적으로 불가능해 더욱 치명적이었다. 이후 현재까지 해운선사를 비롯해 항만 터미널, 선급, 국제해사기구까지 해사 업계에 사이버사고가 다양하게 발생하고 있다(Lim, 2022). 또한 같은 해 2월에는 해적들이 사이프러스를 출항하여 지부티로 항해하는 독일 컨테이너 선박의 항해시스템을 해킹한 사건이 있다. 이 해킹으로 인해 선박은 약 10시간 조종 불능상태가 되었다. 해적은 항해시스템을 해킹하여 선박을 조종하고 자신들이 원하는 장소로 선박을 유도하여 탈취할 계획이었다고 한다(Asiaeconomy, 2022).

한편 해상교통관제에 대한 사이버사고는 2011년 발생한 진도 VTS는 시스템 해킹 사건이 있다. 시스템 해킹으로 인해 레이더망이 무력화되어 20일 동안 관제 업무가 불가했다. 당시 VTS망은 해외에서 원격 수리가 가능하도록 인터넷망에 연결되어 있었으며, 누군가가 완도 VTS의 IP망을 통해 진도 VTS로 들어와 시스템이 정지되도록 해킹을 한 것이다(YTN, 2014). 진도 VTS 관제구역은 신안 도초면을 비롯해 대흑산도, 제주 추자군도, 해남 어란 진을 연결하는 내측 해역으로 면적은 3,800km^{2}로 제주도 면적의 약 2.2배 수준이다. 관제구역의 감시 마비는 국가 안보를 위협하는 치명적인 사건으로 기록되었다.

3.2 국제기구 논의 현황

(1) 국제해사기구

국제해사기구(IMO)는 IMO 전략계획(2018-2023)에서 사이버 보안 기술이 핵심사항이라 공표한 바 있으며, 2017년 6월 개최된 제98차 해사안전위원회에서는 해상 사이버 리스크 관리에 관한 결의서가 채택되었다. 해당 결의서에서는 각 기국은 2021년 1월 1일 이후 도래하는 첫 번째 국제안전관리규약(ISM)의 심사를 수검하기 전까지 각 해운선사에는 사이버 리스크 관리 규정을 선박안전관리시스템(SMS)으로 통합관리할 것을 권고하고 있다(IMO, 2017a). 사이버위협 및 취약점으로부터 비지니스를 보고하기 위한 해상 사이버 리스크 관리 지침을 발표했으며, 관리를 위해서는 인식, 보호, 탐지, 대응 및 복구에 대한 요소를 권고토록 정하고 있다(IMO, 2017b).

(2) 국제항로표지협회

국제항로표지협회(IALA)는 항행 지원시설의 사이버 보안에 대해 논의하기 시작했으며, 2021년에는 사이버 보안 워크숍을 개최하였다(IALA, 2021). 워크숍에서는 사이버 보안과 인적요소, IALA 범위 내 플랫폼 및 시스템, 사이버 사고 대응 및 복구에 대해서 논의했다. 해당 워크숍을 통해 IALA는 선박의 디지털화에 따라 항행 지원시설의 보안이 중요한 요소임을 확인했으며, 지속적으로 논의해 나갈 것이라 했다.

한편 중국 MSA는 VTS도 사이버 사고에 대비할 필요가 있다고 주장하였다. VTS 시스템은 레이더, AIS, CCTV, VHF 등과 같은 데이터를 활용하며, 타 관련 기관 및 도선, 항만, 수색 및 구조 부서 등과 정보를 공유하고 있다. 그러므로 VTS 시스템은 더 많은 네트워크 경계와 데이터 교환 인터페이스를 가지며 결과적으로 사이버 위험이 다른 시스템보다 높다고 했다. 특히 VTS 시스템은 다수의 선박 파일, 항해 데이터, 교통 데이터를 저장하며 그 중 일부는 기밀 보장이 필요한 정보이기 때문에 유출 시 심각한 문제가 발생할 수 있다고 했다.

(3) 국제선급협회

국제선급협회는 지난 2016년 선박 내 사이버 사고가 인명, 재산 및 환경에 심각한 영향을 미칠 수 있음을 인식하여 사이버 이슈를 체계적으로 논의하기 위해 사이버시스템 패널을 신설했다(Lim, 2022). 그리고 신조선과 선박에 탑재되는 기자재 시스템 사이버 보안 통합 요구사항(Unified Requirement: UR)을 수립하고 이를 바탕으로 2024년 각 선급에서는 선박 건조 시 조선소 및 제조사에 사이버 보안 관련 요건 준수를 강제화 할 예정이다. 신조선 통합 요구사항의 목표는 설계, 건조, 시운전 및 운영 등 전 주기 동안 운영기술 및 정보기술 시스템을 효과적으로 관리하는 것이다(IACS, 2022a). 기자재 시스템은 시스템 무결성이 제조사에 의해 보호, 강화되도록 하는 것이 목표이다(IACS, 2022b).

3.3 산업계 논의 현황

(1) 선주단체

발트국제해사협의회(BIMCO)는 선주단체에서 선박 사이버 보안에 대한 적용지침(4판)을 2020년에 발표하였다. 이 지침에는 선주 및 운영자에게 회사 및 사이버시스템의 보안을 유지하기 위한 절차 및 조치에 대한 지침을 제공하고 있다. 고위경영진은 조직의 레벨과 부서에 사이버 위험 인식문화를 포함해야 하며, 효과적인 피드백 메커니즘을 구성하여 유연한 관리체계를 보장해야 한다고 명시하고 있다(BIMCO, 2020).

(2) 화주협회

OCIMF는 화주가 직접 사이버 보안 검사기준을 개정하여 국제변화에 대응하고 있다. 탱커선 운항 선사 안전관리 평가 기준 3판에서는 2018년 1월부터 탱커 선박을 보유하고 있는 선사에 대하여 사이버 보안 정책서, 절차서 이행, 리스크 평가수행, 임직원 인식 제고 교육 등을 포함한 17가지 항목을 설정하고 사이버 보안 관리 능력을 점검한다. 또한 탱커 안전성 평가 기준(SIRE VIQ) 7판은 사이버 보안과 관련한 사용자의 책임과 역할, 선박의 OT/IT 시스템의 식별, 사이버 위험을 방어하기 위한 기술적인 방안, 절차 등 4개 항목을 점검하도록 제시하고 있다(OCIMF, 2022).

4. VTS 인원 대상 설문조사

4.1 설문조사 개요

VTS의 해상 사이버 보안 대응 현황을 살펴보고, 정책 우선순위를 도출하기 위해 VTS 인원을 대상으로 설문조사를 수행하였다. VTS 인원은 관리자(센터장), 관제사, 행정/시설, 정보보호 분야로 구성되어 있으므로(Yoo et al., 2018) 역할을 고려하여 설문조사를 수행했다. 설문조사는 2022년 10월 24일부터 28일까지 총 5일간 진행되었으며, 전국의 VTS 인원 30명이 참여했다. Fig. 1은 설문에 참여한 VTS 인원의 업무 영역을 나타낸다. 관제사가 59.4%로 가장 많았으며, 시설 담당, 정보보안 순으로 참여했다.

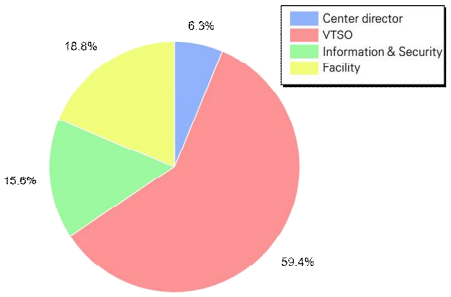

Fig. 1. Survey participant.

4.2 분석 방법론

KMI(2019)는 ISO/IEC 27001 부속서 A의 관리적, 기술적, 물리적 보안 분야 통제항목과 선주단체에서 제시한 기술적, 관리적 보안 분야의 통제항목을 고려하여 위험 요소를 도출한 바 있다. 그리고 통제 실패 시에 위험 요소를 우선순위로 식별했으며, 본 연구에서는 위험 요소 중 우선순위가 높게 식별된 요소를 활용하여 VTS 중심의 사이버 보안 정책 우선순위를 살펴보고자 했다. Table 2은 설문조사에 사용될 각 보안 분야별 취약성 개선 요인을 나타낸다.

Table 2. Risk factors by security area

Security Area	Risk factors in case of control failure	
Administrative security	1	Raise awareness and train employees on how to protect information
	2	Control the use of portable media (USB, portable PC etc)
	3	Maintenance of S/W tools such as H/W, S/W upgrades and anti-virus (V3, etc.)
	4	Establish emergency plans for cyber- attacks
Technical Security	5	Restrict and control access to network ports, protocols, and services (such as login password settings)
	6	Detect, block, and warn against cyber-attacks through the system
	7	Control remote and wireless access by using encryption key (ex. WiFi)
	8	Support data backup and recovery function

Security Area		Risk factors in case of control failure
Physical Security	9	Set physical security zone and control access
	10	Ban on carrying out any equipment, information and software outside without prior approval
	11	Ensure continuous availability (emergency power supply, etc.) and integrity (sensor connection, etc.) of equipment
	12	Confirm removal of data and S/W license when discarding equipment including storage media

보안 분야별 취약성 개선요인은 IPA 분석을 통해 우선순위를 결정한다. IPA 분석은 주요 속성의 중요도와 만족도 간의 연관성을 비교평가 한다(Martilla and James, 1977). 분석의 주요 속성이 결정되면 설문조사를 통해 데이터를 수집하고 수집된 데이터를 사용하여 사분면 형태의 매트릭스를 생성한다. 매트릭스의 X축은 속성의 중요도이며, Y축은 속성의 만족도이다. 매트릭스는 총 사분면으로 구성되어 있으며, 1사분면은 현재 상태를 유지하기 위해 지속적인 관리가 필요한 지속유지영역이다. 2사분면은 과잉 노력 영역으로 중요도는 낮지만 성과는 높은 영역이다. 3사분면은 우선순위가 낮은 구간으로 더 많은 투자가 필요하지 않은 영역이다. 4사분면은 가장 집중적인 노력이 필요한 부분으로, 사용자들이 현재 서비스에 만족하지 못하기 때문에 가장 집중적인 투자가 필요한 부분이다. Fig. 2는 각 사분면이 의미하는 바를 도식화했다.

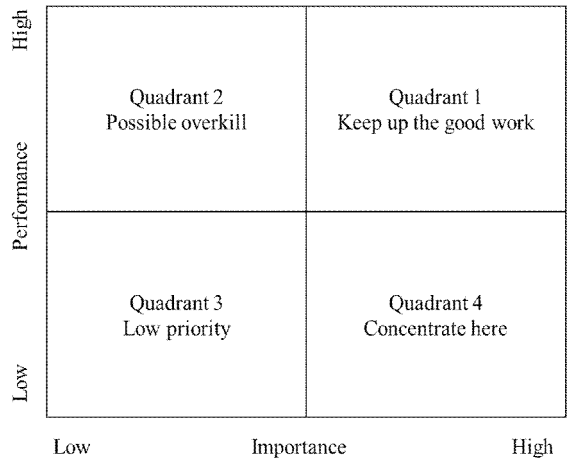

Fig. 2. The standard IPA chart.

본 연구에서는 IPA 분석을 위해 VTS 인원에게 Table 2의 관리적, 기술적, 물리적 보안의 취약성 개선요인을 대상으로 중요도와 만족도를 질의했다. 답변은 리커트 5점 척도로 수집했으며, 각 요인의 점수를 산술평균하여 도출하였다.

4.3 설문조사 결과

(1) 보안업무 경험 유무

VTS는 선박 관제가 주요 업무이기 때문에 관제사가 많으며, 정보보호와 관련된 인원은 별도로 존재한다. VTS는 「정보통신기반 보호법」 제8조에 따라 주요정보통신기반시설로 지정되어있으며, 각 센터는 정보보호 전담 인력을 두고 있다(KCG, 2017). 정보보안과 선박 관제는 분야가 다르기 때문에 보안업무 경험을 기준으로 경험이 있는 그룹과 경험이 없는 그룹을 나누어 분석하고자 한다. Table 3는 업무영역과 보안업무 경험을 나타내는 표이다. 보안업무는 주로 정보보호나 시설에서 담당하고 있었으며, 관제사 대부분은 보안업무에 대한 경험이 없는 것으로 조사되었다. 사이버 공격을 경험한 질문에는 총 5명이 응답했으며, 랜섬웨어, 악성코드 감염, 피싱 및 웹 해킹을 경험했다고 응답하였다.

Table 3. Working area and Security working experience

Working experience / Working area	Yes	No	Total
Center director	1	1	2
VTS Operator	2	17	19
Information protection	5	-	5
Facility	3	1	4
Total	11	19	30

(2) 보안업무 수행현황

관리적, 기술적, 물리적 분야별 사이버 보안 취약성 개선요인의 수행 여부를 조사하였다. Table 4은 분야별 수행현황을 나타낸다. 수행 항목에 대한 결과는 보안업무 경험 유무에 따라 다르게 나타났다. 보안업무 경험이 있는 인원은 상대적으로 보안업무 경험이 없는 인원에 비해 수행 현황을 높게 평가했다. 특히 관리적 보안에서는 '인식 제고 및 교육', '이동 미디어 통제', 기술적 보안에서는 '네트워크 접근 제어', '데이터 백업 및 복구', 물리적 보안에서는 '보안 구역 통제', '정보 반출금지'가 높게 나타났다. 보안업무 경험이 없는 인원은 물리적 보안 중 '보안 구역 통제', '정보 반출금지' 수행 현황이 높게 평가되었다. 이는 직접적으로 겪는 요인이기 때문인 것으로 판단된다.

Table 4. Implementation of cyber security vulnerability improvement factors

Security area	Risk factors	Security work experience		No Security work experience	
		Persons	Rate (%)	Persons	Rate (%)
Administrative security	Raise awareness	9	81.8	8	42.1
	Portable media control	9	81.8	6	31.6
	H/W, S/W upgrade	8	72.7	8	42.1
	Contingency plan	6	54.5	7	36.8
Technical Security	Network control	9	81.8	7	36.8
	Detection cyber attacks	4	36.4	8	42.1
	Wireless access control	6	54.5	6	31.6
	Data back-up	9	81.8	8	42.1
Physical Security	Physical security area	10	90.9	10	52.6
	Access control	10	90.9	10	52.6
	Secure continuous availability	7	63.6	7	36.8
	confirming removal	3	27.3	3	15.8

(3) 중요도-성취도 분석 결과

보안업무 경험이 있는 인원의 IPA 분석 결과, 1사분면 지속 유지영역은 '인식 제고 및 교육', '네트워크 접근 제어', '보안 구역 통제'로 나타났다. 2사분면 과잉영역은 'USB 등 미디어 통제'로 나타났다. 'H/W, S/W 업그레이드', '비상계획 수립', '원격/무선 접근제어', '데이터 백업 및 복구', '장비 가용성/무결성 보장', '데이터 및 라이센스 폐기' 등은 우선순위가 낮은 요소로 나타났다. 4사분면 집중투자 영역은 '사이버 공격 탐지 및 차단', '정보 및 S/W 반출금지'로 나타났다. Fig. 3은 IPA 분석 결과를 매트릭스에 도식화한 것이다.

사이버 보안 취약성 개선요인 현황과 함께 분석하면, '사이버 공격 탐지 및 차단' 요소는 현재 수행이 낮은 상태이며, IPA 분석에 따른 집중투자 영역으로 분석되어 최우선으로 추진되어야 할 요소로 판단된다.

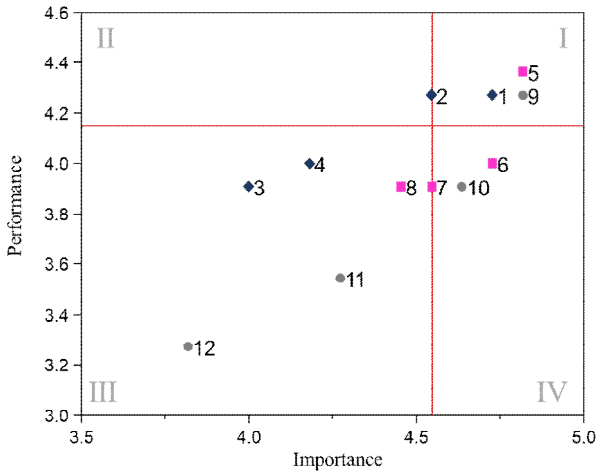

Fig. 3. Result of personnel with experience in security work.

보안업무 경험이 없는 인원의 IPA 분석 결과, 2사분면 과잉영역에는 '인식 제고 및 교육'이 있으며, 우선순위가 낮은 3사분면에는 '미디어 통제', '데이터 및 라이센스 폐기' 가 분포 했다. 4사분면의 집중투자 영역은 없었으며, 나머지 요소는 모두 1사분면에 분포하고 있었다. 보안업무 경험이 없는 인원은 사이버 보안 취약성을 개선하기 위한 요소들이 현재에도 대부분 잘 수행되고 있다고 판단하고 있으며, 추가로 개선하고 집중 투자해야 할 부분은 크게 없는 것으로 인식하고 있다. Fig. 4는 IPA 분석 결과를 매트릭스에 도식화한 것이다.

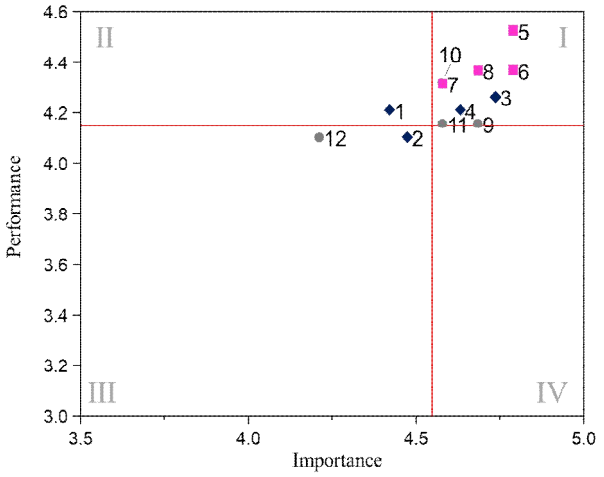

Fig. 4. Result of personnel without experience in security work.

보안업무 경험이 없는 인원은 대부분 관제사로 해상교통상황 파악 및 정보제공, 해양사고 예방을 위한 선박관제, 항만 운영 정보 제공 등의 역할을 수행하고 있다. 그러므로 보

안업무에 대해서는 잘 인식할 수가 없으며, 직접적인 교육이나 물리적인 접근제어 등의 보안 관련 사항만 파악할 수 있다. 이는 사이버 보안 취약성 개선요인의 수행현황에서도 파악할 수 있다. 또한 관제사 대상 인터뷰 결과 사이버 보안에 대한 용어가 생소하다는 의견도 있었다.

4.4 고찰

본 연구에서는 VTS 인원 대상 설문조사를 통해 사이버 보안 취약성 개선을 위한 활동 현황과 우선시 되어야 하는 요소들을 식별하고자 했다. 그리고 효과적인 결과 분석을 위해 사이버 보안 담당의 경험 유무에 따라 구분했다. VTS는 정보통신기반 보호법에 따른 주요정보통신기반시설이기 때문에, 센터마다 정보보호 담당 인력이 있으므로 사이버 보안 담당의 경험이 있는 인원은 주로 정보보호 담당이나 시설 담당이었다.

분야별 사이버 보안 취약성 개선요인에 대하여 보안 담당자 입장에서는 '데이터 및 라이센스 폐기', '사이버 공격 탐지 및 차단'을 제외하고는 절반 이상이 수행하고 있다고 답했다. 반면 보안업무 경험이 없는 입장에 서는 '보안 구역 통제', '정보 및 S/W 반출 금지'를 제외하고는 대부분 수행하고 있지 않다고 답하였다. 특히 '인식 제고 및 교육'도 42.1 %만 수행하고 있다고 응답했다. 보안업무 경험이 있는 인원은 사이버 보안과 관련하여 활동하고 있지만, 경험이 없는 인원은 이에 대한 관심이 떨어지는 것을 확인할 수 있다.

IALA(2021)는 사이버 보안 워크숍에서 사이버 보안의 인적요소에 대하여 논의했다. 논의 결과는 일상생활에서 전 직원에 대해 사이버 보안 인식을 높일 필요가 있으며, 사이버 보안 관련 역할 및 책임은 조직 전반에 할당되어야 한다고 했다. 설문조사 결과에 따르면, 현재는 보안 담당자와 비담당자 간에 사이버 보안에 관한 인식이 차이가 있는 것으로 판단되며 조직 전체에 사이버 보안에 대한 인식을 개선할 수 있는 정책이 필요하다.

보안담당자 응답에 대한 IPA 분석 결과, 기술적 측면에서 '사이버 공격 탐지 및 차단', 물리적 측면에서는 '정보 및 S/W 반출금지'가 집중적으로 투자되어야 할 요소로 도출되었다. IALA(2021)의 워크숍에서는 AIS와 GNSS에 대한 위협을 저지할 방안 고려가 필요하다고 했다. VTS는 선박 관제를 위해서 항상 선박의 AIS 신호를 감시하고 있으며, 사고 발생 시 가장 우선적인 대응이 필요하다. 그러므로 사이버 공격 및 차단에 대한 기술개발 및 VTS 상황에 맞는 적용이 필요하며, 이러한 조치는 사이버 공격에 대한 선제적 조치로 2차, 3차의 피해를 방지할 수 있으리라 판단된다.

5. 결 론

4차 산업혁명의 물결에 따라 해운업계의 패러다임은 크게 변화하고 있으며, 선박에는 정보 통신 기술이 적용되어 운영 중이던 항해 장비들이 디지털화 되거나, 선박과 선박 그리고 육상 간의 통신망 연결이 가속화되고 있다. 이러한 변화는 사이버 보안 위협의 증가를 야기한다. 본 연구는 해상교통관제 분야에 사이버 보안과 관련된 현황과 필요한 정책을 제언하고자 했다. 연구 결과로 도출된 내용을 요약하자면, 다음과 같다.

(1) IMO는 사이버 위험 관리를 ISM에 반영하도록 권고했으며, 국제선급협회는 신조선과 탑재되는 기자재에 대해 요구사항을 수립하고 이를 강제화했다. 선박분야에서는 이미 현실화된 사이버 위협을 대비하기 위한 규정이 개발되며, 적용되고 있다. 해상교통관제는 육상지원시설로 선박과의 연결이 불가피하므로 이에 대한 대비책 마련이 시급하다.

(2) VTS 인원을 대상으로 사이버 보안 현황과 정책 우선순위를 도출하기 위한 설문조사를 수행했다. 설문조사 결과 사이버 보안 정보 담당인원과 비담당인원의 인식 차이는 큰 것으로 나타났다. 사이버 보안은 조직의 전 인원이 심각성을 인지하고 대응해야하므로 이에 대한 조치가 필요하다.

(3) IPA 분석결과 사이버위협 탐지 및 차단 요소가 기술적으로는 가장 투자가 필요한 요소로 도출되었다. 물리적 영역에서는 정보 및 S/W 반출금지의 투자가 필요하다고 도출되었으며, 이 두 요소를 위한 정책이 우선 수립되어야 할 것으로 판단된다.

본 연구는 해운분야 디지털의 가속화에 따른 VTS 입장에서 사이버 보안 관리를 위한 제언을 하였다. 설문조사에 참석한 VTS 인원은 30명으로 많은 인원의 의견을 듣지 못한 것이 본 연구의 한계점이다. 추후에는 연구를 통해 도출된 요소를 구체화 시키고, 시나리오 별로 VTS가 대응해야하는 지점과 방안에 대해서 연구를 이어나갈 예정이다.

Acknowledgement

This research was supported by the 'Development of Autonomous Ship Technology(20200615)' funded by the Ministry of Oceans and Fisheries(MOF, Korea).

References

[1] Asiaeconomy(2022), Hacking threat rises in the age of autonomous ships, https://www.asiae.co.kr/article/industry-IT-all/

2022102514515879797 (Assessed in 1st Nov. 2022).

[2] BIMCO(2020), The Guidelines on Cyber Security Onboard Ships, Ver. 4.

[3] Chang, M. H. and D. Y. Kang(2012), Factors Affecting the Information Security Awareness and Perceived Information Security Risk of Employees of Port Companies, Journal of Navigation and Port Research, Vol. 36, No. 3, pp. 261-271.

[4] D'agostini, E. and S. H. Jo.(2019), Maritime Security Training: Evaluation of the Impact on Seafarers' Security Awareness and Security Performance, Journal of the Korean Society of Marine Environment & Safety, Vol. 25, No. 2, pp. 201-211.

[5] D'agostini, E., D. K. Ryoo, and S. H. Jo.(2017), A Study on Korean Seafarer's Perceptions Towards Unmanned Ships, Journal of Navigation and Port Research, Vol. 41, No. 6, pp. 381-388.

[6] IACS(2022a), Cyber resilience of ships

[7] IACS(2022b), Cyber resilience of on-board systems and equipment

[8] IALA(2021), Report of the workshop on Cyber security.

[9] IMO(2017a), Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems.

[10] IMO(2017b), MSC-FAL.1-Circ, Guidelines on Maritime Cyber Risk management.

[11] KCG(2017), Final report on research for coastal VTS intergration effect analysis.

[12] Kim, G. E.(2022), System Improvement Plan for Vessel Traffic Service(VTSO) Education and Training Following the Emergence of Autonomous Vessels, Jonrnal of Korean Maritime Police Science, Vol. 12, No. 3, pp. 69-99.

[13] Kim, H. T. and Yang, Y. H.(2019), A review of Human Element Issues of Remote Operators on Maritime Autonomous Surface Ships, Journal of Navigation and Port Research, Vol. 43, No. 6, pp. 395-402.

[14] KMI(2019), A Study on Strengthening Cybersecurity System in the Maritime Sector, Korea Maritiem Institute

[15] Lee, E., Y. J. Ahn, and S. H. Park(2020), A Study on the Development of a Training Course for Ship Cyber Security Officers, Journal of the Korean Society of Marine Environment & Safety, Vol. 26, No. 7, pp. 830-837.

[16] Lim, J. K.(2022), Maritime Cyber Security International Classification Association Trends, Weekly ICT Trends, Institute of Information & Communications Technology Planning & Evaluation, pp. 2-12.

[17] Martilla, J. A. and J. C. James(1977), Importance-Performance Analysis, Journal of Marketing, Vol. 41, No. 3, pp. 77-79

[18] OCIMF(2022), SIRE 2.0 Question Library Part 1.

[19] Park, S. W., Y. S. Park, H. S. Park, and Y. J. Yoo(2020), A Study on the Improvement of VTS System by the Introduction of Maritime Autonomous Surface Ship(MASS), Journal of Korean Maritime Police Science, Vol. 10, No. 4, pp. 19-50.

[20] Yoo, S. L., Y. G. Lee, and C. Y. Jung(2018), A Study on the Information Security of VTS, Journal of Korean Maritime Police Science, Vol. 8, No. 1, pp. 113-128.

[21] YTN(2014), Jindo VTS hacking accident, https://www.ytn.co.kr/_ln/0103_201404271821112463 (Assessed in 1st Nov. 2022).

Received : 2022. 11. 04.
Revised : 2022. 12. 07.
Accepted : 2022. 12. 28.