스마트항만 사이버보안 시스템 활성화 방안

조규성*
동명대학교 항만물류시스템학과 교수

Revitalization of Smart Port Cybersecurity System

Gyusung Cho*
Professor, Department of Port Logistics System, Tongmyong University

요 약 한국 수출입 물동량의 99.7%는 해상을 이용해서 수행되는 만큼 수출입 분야에서 해상운송은 매우 중요한 역할을 하고 있다. 특히 해상운송의 거점인 항만터미널은 해상운송의 시작점이자 종착지로서 효율적인 해상운송을 위한 중요 시설이다. 정부에서도 해상운송의 중요성을 인식하여 항만터미널의 효율성 향상을 위해 사물인터넷 등의 스마트기술을 적용한 스마트항만으로의 전환을 추진하고 있고 일부 항만은 이미 스마트항만터미널로 구축 및 운영이 되고 있다. 현재 국내 항만은 중요 물류 시설이자 국가기반시설로 지정되어 국가차원에서 관리하고 있다. 하지만 항만터미널은 운영주체의 특수성으로 인해서 국가차원에서 보다 효율적인 관리 및 운영에 한계가 있다. 뿐만 아니라 급증하는 사이버해킹 등의 사이버보안위험에 대처하기 위한 항만터미널의 체계적인 사이버보안 구축 및 적용이 필요하다. 이에 본 연구에서는 항만터미널 특히 스마트항만에서 필요한 사이버보안관리 체계 구축 및 운영에 관한 연구 수행을 주요 목적으로 하고 있다. 이를 위해서 국내 항만 현황 및 항만터미널 연계 항만사이버보안체계 구축 방안을 제시함으로써 스마트항만의 사이버보안의 활성화를 주요 목적으로 하고 있다. 본 연구를 통해서 스마트항만 항만사이버보안 시스템의 활성화 및 실제 스마트항만에 적용될 경우 스마트항만의 효율적인 사이버보안이 가능할 것으로 판단된다.

주제어 : 항만터미널, 스마트항만, 사이버보안, 시스템 활성화, 사물인터넷(IoT)

Abstract More than 99% of Korea's import and export volume is carried out by sea, so maritime transport plays a very important role in the import and export sector. In particular, port terminals, which are the hubs of maritime transport, are important facilities for efficient maritime transport as the starting point and end point of maritime transport. The government also recognizes the importance of maritime transport and is considering converting port terminals to smart ports by applying smart technologies such as the Internet of Things to improve the efficiency of port terminals, and some ports are already constructing and operating smart port terminals. Currently, domestic port terminals are designated as important logistics facilities and national infrastructure facilities and are managed at the national level. However, port terminals are operated by individual companies, so there are limitations in more efficient management and operation at the national level. In addition, systematic cybersecurity of port terminals is necessary to deal with cybersecurity risks such as cyber hacking that are rapidly increasing. Therefore, the main purpose of this study is to conduct research on the construction and operation of a cybersecurity management system required for port terminals, especially smart ports. In this paper, we show the current status of domestic port terminals and the establishment of a port cybersecurity system linked to port terminals are presented, with the main goal of activating cybersecurity in smart ports. Through this study, it is believed that efficient cybersecurity in smart ports will be possible through the activation of the port cybersecurity system in smart port terminals and the application of actual smart ports.

Key Words : Container Terminal, Smart Port, Cybersecurity, System Revitalization, Internet of Things (IoT)

This Research was supported by the Tongmyong University Research Grants 2024(2024A020)
*교신저자 : 조규성(gscho@tu.ac.kr)
접수일 2025년 07월 07일 수정일 2025년 08월 11일 심사완료일 2025년 08월 21일

1. 서론

항만물류의 가장 중심적인 역할을 수행하고 있는 곳은 항만터미널로서 해상/항만에서 발생되는 수출입화물의 물류흐름과 관련된 제반 업무를 수행하는 곳이다[1-2]. 항만터미널은 효율적인 항만시설 계획 및 운영을 위해 대형화되고 있는 컨테이너 선박의 재항시간을 단축시켜야 하는 상황에 처해 있다. 이를 위해 항만터미널의 하역시스템 자동화, 운영시스템 고도화, 항만터미널 시설물의 재배치 등을 통해서 항만터미널 생산성 향상을 위한 노력을 수행하고 있다[3-4]. 국내 항만은 무역항 및 연안항으로 구분하고 있으며, 무역항과 연안항은 국가관리항 및 지방관리항으로 지정하고 있으며, 국내 62개항 중 무역항은 31개항 및 연안항은 31개항으로 구성되어 있으며, 무역항은 910개 선석 및 연안항은 123개 선석으로 구성되어 있다[5]. 항만터미널은 무역항에 설치되어 있으며 주로 부산항, 광양항, 인천항, 울산항, 마산항, 평택•당진항에서 운영되고 있다. 뿐만 아니라 해양수산부에서는 부산항 신항 7부두를 2024년도에 완전 자동화 항만 개장 및 2030년 완전 무인화 조성 추가 운영 계획 등 스마트 항만 기술 산업 육성 사업을 추진하고 있다[6]. 이에 신규 항만터미널의 무인화/자동화에 따른 항만터미널의 '생산성 향상' 및 '안전성 강화' 목적으로 ICT(Information and Communications Technology) 등 첨단 기술을 적용한 스마트항만 통합유지 운영시스템을 개발하여 첨단 해양 분야의 안전관리 체계 확산이 요구되고 있다. 스마트항만은 IoT(Internet of Things), AI(Artificial Intelligence) 등 신기술과 혁신을 통한 물류 최적화, 효율적 에너지 사용, 친환경, 배후도시와 연계강화 등 항만의 포괄적인 기능 및 역할이 포함된 개념이다[7]. 이에 국내에서는 항만터미널의 스마트항만 전환에 따른 무인화 및 스마트화를 통한 사이버보안의 중요성이 증대되고 있다. 사이버보안에서는 IT(Information Technology) 보안기술 뿐만 아니라 OT(Operational Technology) 보안기술도 중요성이 증대되고 있다. 그 이유는 지금까지는 외부에서의 접근이 통제되는 폐쇄성으로 인해 OT 보안에 대한 보안중요성이 적었으나, 디지털화의 진행과 함께 IT 영역과의 접점이 확대되면서 OT를 대상으로 한 사이버 공격이 증가하고 있기 때문이다. 하지만 현재 사이버보안분야에서도 IT보안 분야에 집중하고 있기 때문에, OT보안에 대한 연구나 투자 등은 부족한 상황이다. 즉 IT에 비해 상대적으로 공격루트가 다양하고 보안이 취약한 OT의 사이버보안은 매우 중요한 분야로 부각이 되고 있다[2]. 4차 산업기술의 발달과 코로나 19로 인한 디지털 전환 가속화로 인해서 항만 시설에 대한 사이버 공격이 증가하고 있다. 지속적으로 국가 주요 기반시설이나 주요 산업 보안을 위협하는 대규모 사이버 공격 시도가 지속될 것으로 전망되며, 항만 분야의 ICT 기술 적용에 따라 해킹 공격이 본격화될 것으로 전망되고 있다[8-9]. 하지만 지금까지 국내에서는 항만터미널의 보안은 물리적보안 중심으로 수행되고 있기 때문에 물리적보안 뿐만 아니라 항만터미널의 사이버보안으로의 확대를 통한 보다 체계적인 구축이 필요한 상황이다. 이에 본 연구에서는 스마트항만 사이버보안 시스템 구축 및 활성화 방안 제시를 통한 스마트항만의 보다 안전한 운영을 주요 목적으로 한다.

2. 항만터미널 사이버보안 운영 현황

2.1 항만터미널 항만장비운영 현황

항만터미널 항만장비는 항만터미널에서 컨테이너를 운반하는데 사용되는 장비로서 스마트항만으로 전환에 따라 항만장비는 무인화 및 자동화로 전환이 되고 있다. 주요항만장비는 컨테이너크레인(Container Crane, C/C 또는 Ship-To-Shore Crane, STS Crane), 야드크레인(Transfer Crane, T/C), 자동이송장비(Automatic Guided Vehicle, AGV)가 있다. 국내에서 컨테이너크레인은 211대가 운영되고 있으며, 야드크레인은 658대 및 자동이송장비는 60대가 운영이 되고 있다. 특히 항만터미널 변화에 따라 컨테이너크레인, 야드크레인은 사람의 탑승으로 조작하는 유인하역장비에서 무인하역장비로의 도입이 증대되고 있다.

2.2 스마트항만

스마트항만은 무인화 및 자동화 기반의 기존의 유인항만에서 무인 항만으로 전환된 항만이라고 정의할 수 있다. 하지만 4차산업혁명에 따른 기술변화는 항만분야에도 영향을 미쳐서 기존의 무인화 또는 자동화 기반의 무인항만에서 스마트항만으로의 정의 및 운영의 확대가 필요하게 되었다. 항만의 스마트화를 적극적으로 추진하고 있는 항만으로는 로테르담항, 함부르크항, LA항, 롱비치항, 칭다오항, 투아스항 등이 있다. 먼저 네덜란드 로테르담항은 선박하역작업을 수행하는 컨테이너크레인까지 자동화한 세계 최초의 완전자동화 항만터미널을

2015년 APMT(APM Terminals)와 RWGT(Rotterdam World Gateway Terminal)을 개장한 데 이어 항만의 스마트화를 추진하고 있는 대표적인 항만이다[10]. 스마트항만의 정의는 학자마다 상이하나 국외에서는 지식 개발 및 공유, 운영 최적화, 항만 탄력성 향상, 지속가능개발 주도, 안전과 보안 확보 등을 목표로 하는 항만 및 고학력자, 숙련된 노동력, 지능화된 인프라, 그리고 자동화가 조화롭게 구성된 종합 항만이 스마트항만이라고 제시하고 있다[11]. 또한 국내에서는 IoT, AI 기반의 자동화 장비/기술을 활용해 자동으로 화물을 처리하고 물류 최적화, 친환경 및 에너지 효율화, 배후도시 연계성 강화와 물류망 전체 데이터 수집·가공·분석·공유가 가능한 항만을 스마트항만이라고 제시하였다[12]. 해양수산부에서는 2030년까지 스마트항만 구축을 통한 글로벌 경쟁력 강화 목적으로 「2030 항만정책 방향과 추진전략」을 발표하였다[6]. 「2030 항만정책 방향과 추진전략」은 2030년까지 항만 자동화·디지털화를 본격 추진하며 이를 위해서 광양항에 항만자동화 테스트베드 구축 및 운영, 부산항 신항 및 진해신항에 자동화 기술 도입으로 2030년부터 본격적인 한국형 스마트 항만 운영을 계획하고 있다. 이를 통해 항만의 자동화·디지털화를 통한 스마트 해상물류 기반 마련을 주요 목적으로 한다.

2.3 스마트항만 항만장비

항만터미널 항만장비는 컨테이너 이송과 관련된 운영을 담당하고 있으며, 스마트항만 도입에 따라 항만장비는 스마트항만장비로 개발되어 항만터미널에 적용이 되고 있다. 스마트항만의 대표적인 항만장비는 컨테이너크레인, 야드크레인 및 자동이송장비가 있다. 컨테이너크레인은 Fig.1과 같으며, 부산항 신항 7부두에 국내 최초로 2단계 컨테이너양적하 방식을 적용한 컨테이너크레인이 도입되었다. 본 항만항역장비는 Double Trolley 방식으로 1st Trolley 원격 조종 및 2nd Trolley는 완전자동화로 운영되고 있다. Fig.2는 야드크레인으로 자동이송장비와 장치장간의 컨테이너터 양적하를 담당하는 항만장비이다. Fig.3은 자동이송장비로서 스마트항만내에서 컨테이너를 무인으로 운반하는 무인운반장비이다. 특히 자동이송장비는 차량관제시스템인 FMS(Fleet Management System)와 연동되어 스마트항만에서 컨테이너를 처리하고 있다. 이들 항만장비는 스마트항만장비로서 유선 또는 무선통신을 통한 무인작업을 수행하고 있다.

(Source : www.dgtbusan.com/DGT/)

〈Fig. 1〉 STS Crane

(Source : www.dgtbusan.com/DGT/)

〈Fig. 2〉 ARMG Crane

(Source : www.dgtbusan.com/DGT/)

〈Fig. 3〉 AGV

3. 사이버보안

사이버보안이란 사이버공간에서 위험과 위협, 그리고 범죄로부터 보호하는 것이라고 정의한다[13]. 또한 사이버보안이란 정보보안에서 그 중점을 사이버공간 또는 네트워크 중에서 발생하는 사이버공격 또는 사이버 위협으로부터 정보통신망과 정보의 비밀성 · 무결성 · 이용가능성을 유지하는 것을 지칭하는 것이라 정의하고 있다[14]. 한국인터넷진흥원의 2024년 하반기 사이버 위협 동향분석에 따르면 2023년 1,277건에서 2024년 1,887건으로

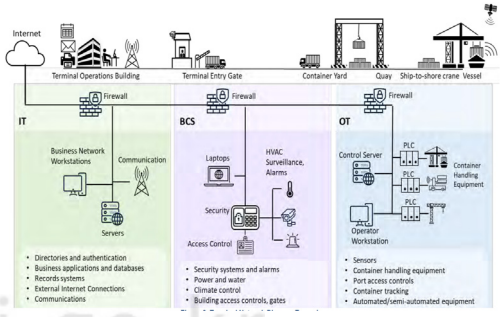
전년 대비 사이버침해사고 신고가 전년 대비 약 48% 증가하고 있다고 발표했다[15]. 특히 서버 해킹(553건)과 정보 유출, 스팸문자 및 메일 발송 등의 유형(180건)이 크게 증가한 것으로 나타났다. 피해가 발생한 업종별로는 정보통신 분야에서 2024년 601건으로 가장 높은 비중을 차지했고, 상대적으로 보안 관리가 취약한 협회 및 단체, 수리 및 기타 개인 서비스업이 2024년 121건으로 전년 대비 약 66%가 증가했다[15]. 사이버보안은 일반적으로 네트워크보안((Network Security), 엔트포인트보안(Endpoint Security), 애플리케이션 보안(Application Security), 클라우드 보안(Cloud Security), 시스템 보안(System Security), 데이터 보안(Data Recovery)으로 구분할 수 있다[16]. 뿐만 아니라 사이버보안은 물리적 보안, IT(Informational Technology) 보안 및 OT(Operational Technology) 보안으로 구분할 수 있다. 물리적 보안은 설비 및 시설 등의 물리적인 접근을 통한 사이버공격에 대응하기 위한 보안대책으로 출입통제, 침입경보, 잠금장치, CCTV 등을 포함한 기술을 말한다. IT 보안은 PC, 모바일기기, 서버 등의 IT 기기로 구성된 영역에서 사이버 공격으로부터 컴퓨터, 네트워크, 소프트웨어, 중요한 시스템, 민감한 데이터 등을 보호하기 위한 보안기술을 말한다. 마지막으로 OT 보안은 제어시스템의 상태 모니터링, 제어, 운용 등에 필요한 제어시스템 대상의 보안위협에 대응하기 위한 보안기술이다. 특히 OT 보안에서는 센서나 모터, 제어기기(PLC, DCS 등), 운영센터(HMI, SCADA 등) 대상의 보안위협에 대응하기 위한 보안대책으로 IT 영역과 달리 운영의 연속성(가용성)이 가장 우선순위가 높은 분야이다[17]. 원자력, 전력 등의 분야에서는 OT 보안 기술개발이 지속적으로 추진 중이나, 항만터미널 내 장비 및 OT 보안 관련 기술개발은 전무한 상황이다. 국내에서도 사이버공격에 대응할 수 있는 다양한 상용기술을 보유하고 있으나 항만터미널 특성을 고려한 사이버보안 기술개발은 매우 부족한 상황이다. 그 이유는 항만터미널은 OT 보안대상이 고정된 타 분야와 달리 AGV 등 보안대상의 자율이동이 가능하고 항만터미널운영시스템(Terminal Operation System, TOS)에 의해 계획/운영되면서, 이상상황 발생 시 현장작업까지 연계됨에 따라 변동성이 매우 크고 복잡한 시스템으로 구성되어 있기 때문이다.

3.1 국내 스마트항만 연계 사이버보안 관련 주요 정책 현황

국내에서는 해양수산부를 중심으로 국제항해에 이용되는 선박과 그 선박이 이용하는 항만시설의 보안에 관한 사항을 정한「국제항해선박 및 항만시설의 보안에 관한 법률」, 「국가물류기본계획」및 「해양수산발전기본계획」등의 관련 정책등을 시행하고 있다. 하지만 항만시설 및 항만하역장비기반 사이버보안 관련 정책은 주로 관련 법령이나 관련 기본계획에서는 사이버보안을 모두 고려하기에는 한계가 있는 것이 현실이다[18]. 또한 국내에서는 항만분야보다는 해사분야의 사이버 보안 관련 활동을 지속적으로 수행되고 있다. 특히 자율운항선박도입에 따른 사이버보안 위협 식별/제시와 사이버보안 강화를 위한 프레임워크 제시 및 항만분야의 컨테이너 인식 진단 관련 연구를 수행하였다[19-20].

3.2 해외 스마트항만 연계 사이버보안 관련 주요 정책 현황

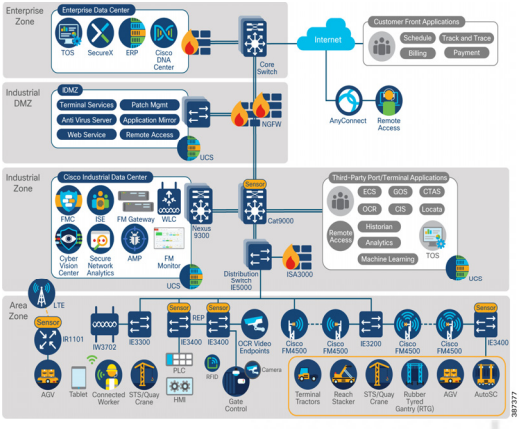
미국의 항만시설은 사이버보안국(CISA: Cybersecurity & Infrastructure Security Agency, USA)을 중심으로 사이버보안을 수행하고 있다. 〈Fig. 4〉는 항만분야 네트워크 구조를 설명하고 있으며 항만분야 보안 관련 업무는 미국 해안경비대를 중심으로 수행되고 있다[21]. 〈Fig. 4〉와 같이 항만터미널의 보안 분야를 IT 보안과 OT 보안을 구분하고 보안별 관리 방안을 제시하고 있다. 또한 미국에서 제시하고 있는 항만분야의 사이버보안 관련 가이드라인을 인터넷을 통해 공개함으로써 누구나 쉽게 접근을 통한 관련 정보를 공유하도록 하고 있다. 유럽에서는 ENISA(European Union Agency for Cybersecurity)를 중심으로 사이버보안 위협 보안 대책 수립 및 운영 방향 제시하고 있다. 〈Fig. 5〉와 같이 항만터미널 운영시스템의 사이버보안 강화 방안 및 관리 체계를 제시하고 있다[22]. ENISA에서는 2019년부터 항만의 사이버보안 관련 가이드라인을 발간하였고, 사이버보안 가이드라인에서는 항만에서 운영되는 자산을 IT와 OT영역으로 구분하여 사이버보안관리 방안을 제시하고 있다.



〈Fig. 4〉 Terminal network diagram

〈Fig. 5〉 Asset taxonomy

뿐만 아니라 세계적인 보안기업체인 CISCO에서도 〈Fig. 6〉와 같이 항만장비를 Area Zone으로 설정하고 항만터미널에서 사용되는 항만장비를 End-to-End 보안 아키텍처의 하위집합으로 선정하여 효율적인 사이버보안을 수행하기 위한 IT 및 OT 영역 통합을 제시하고 있다[23]. 또한 항만터미널운영을 위한 안정적이고 안전하며 효율적인 네트워크 인프라를 설계 및 구현을 수행할 수 있는 아키텍처를 제시하고 있다.



〈Fig. 6〉 Connected ports and terminals

네덜란드 암스테르담항은 항만터미널의 사이버 내성 강화를 목표로 사이버보안 프로그램을 개발하였다. 개발된 프로그램은 핫라인(Hot Line)과 CYREN 네트워크(Cyber Resilient North Sea Canal Area)라는 두 가지 중요 요소로 구성되어, 위협이나 사고에 따른 최신 정보를 신속히 공유함으로써 항만 지역에 대한 사이버보안 강화를 지속적으로 수행하고 있다[24]. 이처럼 해외 국가와 기업체 및 항만터미널에서 사이버보안 구축 및 운영을 위한 다각적인 노력을 수행하고 있다.

4. 스마트항만 사이버보안 강화 방안

스마트항만의 디지털화에 따른 항만터미널의 사이버보안 중요성이 증대됨에 따라 정부차원에서 지속적인 스마트항만의 사이버보안 강화 정책 계획 수립 및 운영이 필요하다. 미국, 유럽, IMO(International Maritime Organization, 국제해사기구), IAPH(International Association of Ports and Harbors, 국제항만협회) 및 ENISA에서는 항만터미널에 적용되는 사이버보안 관련 지침 마련 및 가이드라인을 인터넷 등을 통한 제공하고 있다. 하지만 국내에서는 항만관련 가이드라인이 공개되고 있지 않기 때문에 일반적 항만터미널의 사이버보안 운영을 위한 부분의 가이드라인 공개를 통해 스마트항만 운영사 및 항만장비제조 기업체에서 항만장비의 효율적인 사이버보안 강화에 필요한 기초자료로 활용이 필요하다. 해외에서는 항만시설에 관한 IT 보안 및 OT 보안 관련 기술을 구분하여 관리할 것을 강조하고 있는 것처럼 국내 항만터미널의 보안을 IT 보안과 OT 보안으로 구분하여 각각의 보안기술을 제시하는 것이 필요하다. 뿐만 아니라 네트워크 디바이스 및 항만 자산에 대한 네트워크 관리 및 항만터미널에 대한 이상탐지 등의 네트워크의 사이사보안 강화 방안을 지속적으로 수행해야 될 것이다. 항만시설은 국가기반시설로서 사이버공격으로부터 보호하기 위해서는 국가차원에서 지속적인 항만 사이버보안 연구 및 관련 R&D가 지속적으로 추진되어야 한다. 국내 항만시설보안료는 항만시설소유자가가 항만시설에 경비·검색 인력을 확보하고 보안시설·장비를 설치하는데 실제 투입한 비용에 대해 해당 항만시설을 이용하는 국제항해선박소유자, 여객 및 화주로부터 징수하는 비용이다. 항만시설보안료는 「국제항해선박 및 항만시설의 보안에 관한 법률」에 기반하여 책정되고 있다. 항만시설보안료는 인건비, 유지보수비 및 감각상각비를 모두 포함

하여 산정된다. 하지만 하지만 「국제항해선박 및 항만시설의 보안에 관한 법률」제6조(징수요율)에서는 컨테이너 화물(20피트 기준)은 TEU당 86원으로 2015년 시행 이후 10년 이상 항만시설보안료는 인상이 없는 상황이다. 이에 항만시설보안료 또한 현실에 맞게 인상이 필요하다. 또한 항만터미널의 스마트항만 전환에 따른 항만분야 사이버보안에 대한 관점도 유.무선통신 등 스마트 기술을 고려한 항만보안정책 수립 및 관련 기관과의 지속적인 의견 수립을 통한 수립이 요구된다. 그리고 항만장비 PLC(Programmable Logic Controller)/센싱/HMI(Human Machine Interface) 등의 스마트항만 OT 시스템 구성요소와의 사이버보안 강화 프레임워크 개발 및 제시가 필요하다. 또한 스마트항만 OT 시스템 내의 네트워크 트래픽, TOS 정보 등을 실시간 분석 및 탐지 기술 개발 및 스마트항만 적용이 필요하다.

5. 결론

항만터미널은 해상운송의 시작점이자 종착지로서 수출입을 중요시하는 한국에서는 중요한 위치를 차지하는 시설이다. 특히 항만터미널은 해상교역의 중요한 역할을 수행하는 시설로서 국가차원에서 지속적인 관리 및 운영이 필요한 시설이다. 하지만 그 중요성에 비해서 국내 항만에 대한 사이버보안 강화 노력은 많이 필요한 상황이다. 해외에서는 항만분야 사이버보안에 관한 가이드라인 구축 및 보급을 통한 사이버보안 강화를 지속적으로 수행하고 있다. 스마트항만 사이버보안은 정책뿐만 아니라 사이버보안 시스템 구축 및 운영을 통한 체계적인 관리가 필요한 실정이다. 따라서 본 연구에서는 스마트항만의 사이버보안 필요성을 제시하였고 스마트항만 사이버보안 강화 방안을 정책적, 시스템적 측면에서 제시하였다. 스마트항만의 중요성으로 인해서 스마트항만의 사이버보안 강화를 위한 관계부처 및 관계기관의 협력을 통한 지속적인 항만분야의 항만사이버보안 강화 노력이 요구된다. 그리고 스마트항만 사이버보안 강화를 위한 보다 구체적인 기술적 요소 및 세부운영방향은 차후연구에서 제시할 예정이다.

REFERENCES

[1] G.S.Cho, “Improvements of Security System based on Port Logistics Information System,” Journal of the Korea Society for Fisheries and Marine Sciences Education, Vol. 29, No.4, pp.1032-1042, 2017.

[2] G.S.Cho and K.H.Kim, “A Study on the Policy Status of Port Security Related to Port Container Terminal Linkage,” in Proc. 2024 Conf. of Yeongnam Branch, Korea Institute of Information Security and Cryptology, 2024.

[3] G.S.Cho, “Development of Educational Content for Analyzing Container Terminal Operational Capacity,” Journal of the Korea Contents Association, Vol.7, No.11, pp.239-247, 2007.

[4] B.T.Uyen and G.S.Cho, “Efficiency Analysis of Container Ports in Vietnam Using Stochastic Frontier Analysis,” Journal of Ocean Engineering and Technology, Vol.39, No.1, pp.56-62, 2025.

[5] Ministry of Oceans and Fisheries, Port Operations Manual 2023-2024, 2023.

[6] Ministry of Oceans and Fisheries, 2030 Port Policy Direction and Implementation Strategy, 2020.

[7] Korea Maritime Institute, “Smart Port, Necessity Establish a Roadmap Considering the Entire Logistics Network,” KMI Trend Analysis, Vol.74, pp.1-17, 2018.

[8] Ministry of Science and ICT, 2022 Cybersecurity Threat Analysis and 2023 Outlook, 2022.

[9] SK Shieldus, 2022 Security Threat Outlook Report, 2021.

[10] J.E.Cha, Y.S.Kim, and Y.R.Shin, “A Study on the Development of Port Smartness Index,” The Asian Journal of Shipping and Logistics, Vol.37, No.1, pp.113-140, 2021.

[11] A.Molavi, G.J.Lim, and R.Race, “A Framework for Building a Smart Port and Smart Port Index,” International Journal of Sustainable Transportation, Vol.14, No.9, pp.686-700, 2020.

[12] Y.C.Cho, “A Study on Domestic and International Service Cases of Smart Ports,” in Proc. 2019 Spring Conf. of the Korean Society of Safety and Management Science, 2019.

[13] K.S.Lee, “The Problems and Policy Alternatives of Cyber security in the Network Age,” Journal of Korean Association for Regional Information Society, Vol.9, No.1, pp.109-128, 2006.

[14] P.W.Jung, “A Critical Analysis on the Concept of "Cyber Security",” Yonsei Lex Sapientia Law Review, Vol.2, No.2, pp.1-25, 2011.

[15] Korea Internet & Security Agency, Cyber Threat Trends Report, Second Half of 2024, 2024.

[16] KDB Future Strategy Research Institute, “Trends and Implications in the Cybersecurity Industry,” KDB Monthly Research Bulletin, No.813, pp.29-59, 2023.

[17] EC-Council, IT vs. OT: Understanding the Key Differences in Cybersecurity, 2023.

[18] Ministry of Oceans and Fisheries, Act on the Security of International Navigating Ships and Port Facilities, 2024.

[19] J.Y.Park, C.B.Park, and H.S.Park, "Research for Direction of Maritime Cybersecurity Regulatory Framework," Journal of the Society of Naval Architects of Korea, Vol.62, No.1, pp.25-37, 2025.

[20] T.N.T.Phuong, G.S.Cho, and I.Chatterjee, "Automating Container Damage Detection with the YOLO-NAS Deep Learning Model." Science Progress, Vol.108, No.1, pp.1-21, 2025.

[21] U.S Coast Guard, Maritime Cybersecurity Assessment and Annex Guide, 2023.

[22] European Union Agency for Cybersecurity, Port Cycersecurity, 2019.

[23] CISCO, Network Designs for Connected Ports and Terminals, 2025.

[24] Dry Cargo, Cybersecurity Programme Launched To Increase Amsterdam Port'S Resilience, 2019.

조 규 성(Gyusung Cho) [정회원]

■ 1998년 2월 : 동의대학교 산업공학과(공학사)
■ 2000년 2월 : 동의대학교 산업공학과(공학석사)
■ 2003년 2월 : 동의대학교 산업공학과(공학박사)
■ 2012년 3월 ~ 현재 : 동명대학교 항만물류시스템학과 부교수

〈관심분야〉
물류시스템, 항만물류, 사이버보안, 시뮬레이션