한국항해항만학회지 제47권 제6호
J. Navig. Port Res. Vol. 47, No. 6 : 437-447, December 2023 (ISSN:1598-5725(Print)/ISSN:2093-8470(Online))
DOI : http://dx.doi.org/10.5394/KINPR.2023.47.6.437

부산항 컨테이너 터미널 사이버 보안 강화를 위한 탐색적 연구

하도연* · † 김율성

*한국해양대학교 KMI-KMOU 학연협동과정, † 한국해양대학교 물류시스템공학과 교수

Exploratory Study on Enhancing Cyber Security for Busan Port Container Terminals

Do-Yeon Ha · † Yul-Seong Kim*

**KMI-KMOU Cooperation Course, Korea Maritime and Ocean University, Busan 49112, Korea*
† Logistics System Engineering, Korea Maritime and Ocean University, Busan 49112, Korea

요 약 : 항만 산업의 동향은 적극적인 4차 산업 기술을 도입하여 자동화 항만, 스마트 항만 등 새로운 항만의 형태로 발전하고 있다. 그러나 항만의 발전 이면에는 항만 및 컨테이너 터미널 내 사이버 보안 사고 및 위협 가능성 또한 높아지고 있다. 이에 항만 내 사이버 보안 강화와 관련된 연구가 필수적이나 국내에서 진행되는 관련 연구는 미비한 실정이다. 이에 본 연구는 국내 대표 항만인 부산항 중 가장 4차 산업 기술을 적극적으로 도입하는 컨테이너 항만을 중심 사이버 보안 강화를 위한 요인을 도출하고 향후 강화 방안을 도출하고자 하였다. 연구결과 부산항 컨테이너 터미널 사이버 보안 강화를 위한 요인은 네트워크 구축 및 정책 지원, 교육 표준화 및 인력 양성, 법·제도적 요인으로 분류되었다. 이후 도출된 요인을 바탕으로 다중회귀 분석을 실시하였으며 분석 결과를 바탕으로 향후 부산항 컨테이너 터미널의 안전성 확보 및 강화, 신뢰성 확보 및 강화, 성과 및 만족도 향상을 위한 세부 요인을 도출하였다. 본 연구는 점차 증가하는 항만 및 컨테이너 터미널 내 사이버 보안 공격에 대응하여 부산항 컨테이너 터미널의 사이버 강화를 위한 방향성을 제시했다는 점에서 의의를 지닌다.

핵심용어 : 부산항, 컨테이너 터미널, 사이버 보안, 요인분석, 다중회귀분석

Abstract : *By actively adopting technologies from the Fourth Industrial Revolution, the port industry is trending toward new types of ports, such as automated and smart ports. However, behind the development of these ports, there is an increasing risk of cyber security incidents and threats within ports and container terminals, including information leakage through cargo handling equipment and ransomware attacks leading to disruptions in terminal operations. Despite the necessity of research to enhance cyber security within ports, there is a lack of such studies in the domestic context. This study focuses on Busan Port, a representative port in South Korea that actively incorporates technology from the Fourth Industrial Revolution, in order to discover variables for improving cyber security in container terminals. The research results categorized factors for enhancing cyber security in Busan Port's container terminals into network construction and policy support, standardization of education and personnel training, and legal and regulatory factors. Subsequently, multiple regression analysis was conducted based on these factors, leading to the identification of detailed factors for securing and enhancing safety, reliability, performance, and satisfaction in Busan Port's container terminals. The significance of this study lies in providing direction for enhancing cyber security in Busan Port's container terminals and addressing the increasing incidents of cyber security attacks within ports and container terminals.*

Key words : *Busan port, container terminal, cyber security, factor analysis, multiple linear regression analysis*

1. 서 론

4차 산업혁명은 2016년 세계경제포럼인 다보스포럼에서 발표된 이후 지금까지 다양한 분야에 많은 영향을 미치고 있다. 그 중 특히 해운 및 항만 분야에서의 4차 산업 기술 도입은 점차 가속화되고 있다. 특히 대표적인 4차 산업 기술인 Iot, 빅데이터, AI등을 통하여 항만은 자동화, 스마트 항만 등 점차 새로운 모습의 항만으로 변화하고 있다. 선진적인 항만의 경우 과거부터 지속적으로 4차 산업 기술을 적극 도입 및 활용하고 있으며 이를 통해 현재 완전 자동화 항만 및 컨테이너 터미널을 구축하고 운영하고 있다. 대표적인 선진 항만인 네덜란드 로테르담항의 경우 항만 자동화를 위한 연구개발을 지속적으로 진행하였으며 현재 마스블락트(Maasvlate) 2에 위치한 터미널은 모두 무인 자동화로 운영되고 있다. 중국의 상하이항, 칭다오항과 싱가포르항 또한 모두 IoT, 인공지능 등 4차 산업 기술을 적극적으로 활용하여 선진적인 항만의 모습으

† Corresponding author : 종신회원, logikys@kmou.ac.kr 051)410-4332
* 정회원, ehdudl6091@g.kmou.ac.kr 051)410-4890
(주) 이 논문은 "부산항 컨테이너 터미널 사이버 보안을 위한 요인 분석연구"란 제목으로 "2023 공동학술대회 한국항해항만학회논문집(한국해양대학교, pp.64)"에 발표되었음.

로 발전하고 있다. 국내의 경우 2023년 국내 최초로 부산 신항 2-5단계에 완전 자동화 항만을 개장할 예정이다. 이러한 세계적인 항만의 적극적인 4차 산업혁명 기술을 도입 흐름을 통하여 기술 도입은 항만의 효율성과 경쟁력을 높이는 선택적 수단이 아닌 세계 시장에서의 항만의 도태를 방지하고 지속적인 성장을 위한 항만 운영에 있어 필수적인 변화라고 할 수 있다.

이러한 변화를 통해 새롭게 나타난 스마트, 디지털 항만은 작업 프로세스의 무인화, 자동화를 통하여 항만 운영의 효율성 및 생산성 향상, 실시간 정보 공유, 환경오염 최소화, 운영비 절감 등 긍정적인 효과를 보인다. 그러나 이러한 긍정적 변화에 대비되어 사이버 보안 공격, 소프트웨어 및 시스템 오류로 인한 항만 운영 문제 발생 등이 나타나고 있으며 새롭게 나타난 위험 요인을 살펴보면 대부분 기술 의존도가 높아짐에 따라 도출된 위험임을 확인할 수 있다. 2023년 EU 사이버 보안국(ENISA)이 발표한 내용에 따르면 점차 항공, 해양, 철도, 도로 등 운송 분야를 중심으로 사이버 공격이 나타날 것이며 특히 러시아 - 우크라이나 전쟁으로 운송 및 물류 부문 공격이 크게 증가할 것으로 예상하였다. 실제로 2022년 12월 포르투갈 Lison항은 사이버 공격으로 인하여 항만의 시스템 마비, 선박일지, 화물 정보 등을 도난당하는 사고가 발생하였다. 일본의 최대 항만인 나고야 항만은 2023년 7월 랜섬웨어 공격으로 인하여 항만의 모든 컨테이너 터미널을 통제 및 관리하는 나고야 항만 통합 터미널 시스템에 문제가 발생하였으며 이로 인하여 컨테이너 터미널의 반입·반출 작업이 일시 정지되는 사고가 발생하였다. 국내의 경우 아직 사이버 보안 공격에 직접적인 피해는 아직 없으나 타 항만의 사례를 살펴보았을 때 충분히 국내 항만 또한 피해 항만이 될 수 있다고 판단된다. 이러하듯 전 세계적으로 항만 및 컨테이너 터미널의 기술 의존도가 높아짐에 따라 항만 및 컨테이너 터미널 내 사이버 보안의 강화 방안과 관련된 연구가 매우 필요한 상황이다. 이와 관련하여 국외의 경우 관련 연구가 활발하게 진행되고 있으나 국내의 경우 여전히 미비한 실정임을 확인하였다.

따라서 본 연구는 국내 항만 및 컨테이너 터미널의 사이버 공격에 선제적으로 대응할 수 있는 강화 요인 도출을 목적으로 진행하였다. 연구 대상 항만의 경우 국내 최대 항만인 부산항 중 4차 산업 기술 활용을 통하여 자동화가 빠르게 진행되고 있는 컨테이너 터미널을 대상으로 연구를 진행하였다. 연구를 진행하기 위하여 부산항 컨테이너 터미널 이해관계자를 대상으로 설문조사를 실시하였으며 부산항 컨테이너 터미널 사이버 보안 강화를 위한 세부 요인을 도출하였다. 이후 부산항 컨테이너 터미널의 안전성, 신뢰성, 성과 및 만족도 향상을 위한 세부 요인을 도출하기 위한 다중회귀 분석을 진행하였다. 본 연구는 향후 부산항 컨테이너 터미널의 사이버 보안 강화를 위한 기초자료로 활용될 것으로 기대된다.

2. 이론적 배경 및 선행연구 고찰

2.1 항만 및 컨테이너 터미널 내 사이버 보안 현황

항만은 효율성 증대 및 운영비 절감 등 다양한 긍정적 효과를 위하여 지속적으로 4차 산업 기술을 도입하였다. 이에 따라 새로운 항만의 형태로 발전하고 있으나 그 반면 점차 항만 내 기술 의존도 또한 증가하고 있다. 최근 이러한 항만의 변화와 특징을 악용하여 항만 및 컨테이너를 대상으로 한 사이버 보안 공격 및 사고가 급증하고 있다.

인도의 JNPT(Jawaharlal Nehru Port Trust)에 위치하고있는 JNPCT(Jawaharlal Nehru Port Container Terminal)은 2022년 2월 22일 사이버 공격으로 인하여 관리 정보 시스템인 MIS가 다운되는 사고가 발생하였다. JNPT는 인도 컨테이너 터미널 대표 항만 중 하나이며 인도의 주요 항만 중 컨테이너 화물량의 약 50%를 차지하고 있다. 현재 JNPT는 5개의 컨테이너 터미널을 운영하고 있으며 공격을 받은 JNPCT는 항만 신탁에서 직접 운영되고 있는 컨테이너 터미널이다. JNPCT에서 발생한 사이버 보안은 암호화된 바이러스인 랜섬웨어 공격으로 판단되었으며 이후 인도 정부 및 관련 기관은 항만 운영체계를 복원, 대응책 구축 등 다양한 사이버 보안 공격에 대비한 대응 방안을 마련하고 있다. 포르투갈 리스본 항만에서는 2022년 12월 25일 LockBit으로부터 사이버 공격을 받았다. 리스본항은 유럽에서 가장 접근하기 쉬운 항만 중 하나로, 국가의 경제적 안정과 물류 네트워크의 핵심 요소로서 큰 역할을 하고 있다. 본 사건으로 인하여 항만은 재무 보고서, 화물 정보, 승무원 세부 정보, 항만 문서와 관련된 데이터를 도난당했다. 또한 시스템의 마비로 정상적인 물류 활동과 항만 운영이 중단되는 치명적인 상황이 발생하였다. 해당 사고 이후 정부는 사이버 보안을 강화하기 위한 긴급 대책을 시행하기 위해 노력을 하고 있으며 사이버 보안 시스템 개선을 통한 향후 공격에 대비하고 있다. 이러한 항만 및 컨테이너 내에서 발생한 사이버 공격을 통해 사이버 공격으로 인한 항만의 피해는 좁게는 항만 내의 데이터 유출, 시스템 마비 등이 있을 수 있으나 넓게는 화물의 손실과 같은 물리적 사고, 국가 경제와 안보의 위협까지 악영향을 줄 수 있음을 확인하였다.

국내의 경우 현재까지 항만 및 컨테이너 터미널을 대상으로 한 직접적인 사이버 공격 사례는 없다. 그러나 항만 및 컨테이너 터미널의 운영과 데이터를 관리하는 항만공사를 대상으로 발생된 사이버 공격은 지속적으로 증가하고 있다. 국내 대표 항만인 부산항, 인천항, 울산항, 여수광양항을 관리하는 각 항만공사에 따르면 2018년 4개의 항만공사에 대한 사이버 공격은 41건이였으나, 2022년 227건으로 5.5배 증가 추세임을 확인하였다. 이 중 시스템 권한 획득이 311건으로 가장 많은 피해 유형으로 나타났으며, 정보 유출 44건, 악성코드 35건 등의 순으로 피해 유형이 나타났다. 이러하듯 항만 및 컨테이너 터

미널을 관리하는 항만공사를 대상으로 하는 사이버 공격이 높아짐에 따라 향후 직접적으로 항만 및 컨테이너 터미널을 대상으로 하는 사이버 공격이 발생될 가능성이 있다고 판단된다.

이와 같이 전 세계적으로 항만 및 컨테이너 터미널에서 발생하는 항만 사이버 보안 사고 발생에 따라 전 세계적으로 적극적인 대응 방안을 모색하고 있다. LA 항만의 경우 해운 이해 관계자를 중심으로 워킹 그룹을 구성하여 사이버위협 정보를 공유하고 있다. BPA의 경우 터미널 운영사와 공동으로 사이버보안 협의회를 개최하여 공조 방안을 적극적으로 논의하고 있다. 또한 2019년부터 사이버보안 위협정보 공유, 공동 사이버공격 대응 훈련 등을 진행하고 있다.

2.2 선행연구 고찰

2.2.1 항만 및 컨테이너 터미널 대상 사이버 보안 선행연구

Penttilä and Olli(2016)는 4차 산업 기술의 발전 및 적극적인 도입으로 산업 제어 시스템의 연결성이 급속도로 발전함에 따라 새로운 보안 위협을 만들어냈으며 해상의 부문도 이러한 위협에 속한다고 언급하고 있다. 이에 본 논문은 선행연구 분석 및 공격트리 분석법을 사용하여 자동화 컨테이너 터미널 시스템의 사이버 위협을 탐구하였다. 연구를 수행하기 위하여 문헌 검토를 통한 10가지 위험 범주를 도출하였으며 분석 결과를 통해 사이버 보안의 위협은 시스템 중단부터 넓게는 전문 기관의 강력한 인증 필요, 자동화 네트워크 프로세스의 세부적인 관리 등을 도출하였다.

Chalermpong(2021)는 항만산업 발전이 진행됨에 따라 항만의 운영 및 인프라의 능력, 거버넌스 모델 및 행정 체계의 변화, 전략적 제휴 및 새로운 비즈니스와 같은 변화를 나타내고 있다고 말하고 있다. 특히 최근 들어 디지털 변환의 경우 항만의 주요 변화로 나타나고 있으며 그에 따른 보안 공격 또한 증가되고 있다. 그러나 여전히 많은 국가 및 기관은 사이버 보안 문제에 대한 중요도를 인식하고 있지 않음을 문제점으로 나타냈다. 이에 본 논문은 더욱 활발한 연구가 필요하며 새로운 패러다임의 개발에 많은 투자를 추진해야 한다고 보고 있다. 특히 정책 결정자의 관심이 우선적이며 글로벌 공급망에 적극적인 참여를 통해 국제적인 관점에서 사이버 보안의 문제점을 살펴보고 해결책을 구축할 필요성이 있다고 언급하고 있다.

Bunyamin et al.(2021)는 디지털화로 인하여 점차 각종 서비스 및 인프라 사용이 편리해지고 효율적으로 진행되고 있으나 사이버 보안 및 안전 문제가 또한 발생할 수 있음을 강조하였다. 특히 항만, 공항 등의 중요 인프라의 경우 사이버 공격으로 인하여 심각한 문제를 초래할 수 있다고 밝혔다. 이에 본 연구는 터키에서 운영 중인 컨테이너 항만을 대상으로 한 통합된 사이버 보안 위험 관리 모델 평가 프로세스를 바탕으로 연구를 진행하였다. 연구 결과, 항만 자산의 경우 사이버 보안에 큰 영향을 받을 수 있으며 항만 시설 내 IT 인력들의 인식 및 책임감 또한 제고되었음을 도출하였다. 본 연구를 통해 도출된 결과는 컨테이너 터미널의 사이버 보안을 평가에 있어 평가 네트워크를 구축하였다는 점에서 의의를 지닌다.

2.2.2 타 업종 내 사이버 보안 관련 선행연구

항만 분야를 대상으로 한 사이버 보안에 관한 선행연구의 경우 언급한 바와 같이 사이버 보안에 관한 선행연구가 미비하다고 판단하였다. 이에 의료기기산업, 금융산업, 반도체산업, 에너지 산업 등 타 산업군의 선행연구를 분석하였다.

Song(2013)는 정보화 시대의 가속화로 인하여 사이버 범죄 수가 증가하고 있으며 범죄 수법의 체계화됨에 따라 국가 및 기업의 기반을 위협할 가능성이 높아짐을 언급하였다. 특히 사이버 보안 사고의 피해는 데이터 유출뿐만 아니라 경제적 및 인적 손실로 이어질 수 있어 치명적인 결과를 초래할 수 있다. 현재 사이버 보안과 관련된 법령은 존재하지만 체계적이지 못하며, 효과적인 법 개정이 필요하다는 점이 강조되고 있다. 더불어, 공공 및 민간 부문에서 실질적으로 적용 가능한 제도를 모색하고 위기관리 체계를 구축하여 사이버 보안 범죄에 대응해야 할 필요성이 강조되고 있다. 이에 본 연구는 사이버 테러의 변화에 대응하기 위해 보안 및 수사 기관의 대응 강화 방안을 분석하였다. 이를 통해 사이버 테러에 대한 대응 체계 강화, 국가 간 협력 강화, 현행 법·제도의 보완 필요, 민간 부문에서의 신고 의무화 등 다양한 시각에서 시사점을 도출하였다.

Oh(2014)은 사이버 위험에 대한 대응이 개인이나 특정 기관에서 독자적으로 진행함에 한계가 있음을 파악하였으며 국가 차원의 대응 체계를 구축 필요성을 강조하였다. 본 연구에서는 현재 주요국은 사이버 보안을 국가적 정책으로 채택하여 지속적인 정책 수립과 기술 개발을 진행하고 있으나 국내에서는 아직도 사이버 위험 및 보안 활동이 상대적으로 소극적인 편임을 언급하였다. 따라서 본 논문에서는 국외 보안기관의 활동을 검토하고 국내 보안기관의 활동과 비교 분석을 진행하였다.

Yoon et al.(2015)은 정부와 기업의 디지털 관리 방법을 악용한 사이버 위협이 증가하고 있으며 이에 따라 핵심 기능의 중단, 개인정보 유출 등 심각한 문제가 지속적으로 발생됨을 언급하였다. 이에 본 연구는 2009년 이후 주요 사이버 공격 사례를 비교 분석하였으며 분석 결과를 바탕으로 국내 사이버 보안 관리체계 개선 방안을 도출하고자 하였다. 연구결과 종합대책의 경우 기관별 추진으로 인한 막대한 예산 투자 및 인력 확보 한계 등 문제점을 분석하였다. 이에 향후 사이버 보안 대응 방안을 위하여 사이버 안보 전략 수립 및 실시간 공유 시스템 등 보다 선진적인 대응방안을 제시하였다.

Jung(2018)은 에너지 분야와 관련된 시설의 사이버 보안 문제 발생의 경우 경제적 혼란 초래 및 인적 피해가 초래될 수 있기에 사이버 역량 강화방안의 필요성을 밝혔다. 이에 사이버 보안 대응을 위한 체계 및 전략 등을 비교 분석하였다. 분

석 결과 현재 국내의 경우 타국에 비하여 보안 위협 상황에 대한 대응 능력 체계가 낮은 것으로 판단되었다. 이후 국·내외 주요기반시설의 사이버 보안 규정 및 관리평가 표준에 대하여 비교 분석을 실시하였다. 분석결과 인적보안 물리 및 환경보안, 정보보안조직, 비즈니스 연속성 관리, 통신 및 운영관리 등 향후 에너지 분야에 특화된 관리평가 체계 구축 시 필요한 항목을 도출하였다.

Hong(2019)는 4차 산업혁명 시대의 도래로 초 연결 사회에서의 사이버 위험은 점차 증가하고 있으며 피해 또한 점차 지능화, 고도화, 대규모화로 나타나고 있다고 주장했다. 이에 사이버 보안 피해를 최소화하기 위해서는 분야와 목적별을 구분하지 않고 모든 영역이 실시간 공유체계의 확립이 필요하나 여전히 대응체계의 구축은 진행되지 않고 있다. 이에 본 연구는 사이버 범죄 피해의 최소화를 위하여 사이버 보안 컨트롤타워 설치를 통한 신속한 대응체계를 제안하고 있다.

Lee(2019)는 경제 및 사회적 활동에 있어 인터넷 이용이 보편화됨에 따라 보안과 관련된 이슈가 중요해지고 있음을 언급하였다. 특히 금융기관의 경우 해킹과 같은 범죄의 가장 대표적인 대상 산업이며 최근 사이버 공격의 피해가 급증하고 있다. 이에 본 연구는 사이버 위협에 있어 유연한 대응력과 안정성을 보이는 영국의 사이버 금융 보안 정책을 분석하였다. 분석 결과 영국의 전략은 사이버 보안 인증 제도 실시, 햅동 훈련 시행, 기업 간 정보 공유 프로그램 등 다양한 방면에서의 강화 및 대응책을 수립함을 확인하였다.

Lee(2020)는 4차 산업 기술 발전으로 인하여 스마트 의료 분야 또한 혁신적인 성장이 나타나고 있으며 이러한 변화에 따라 의료기기 및 유전체 해킹 등에서 사이버 보안 문제가 발생하고 있음을 언급하였다. 특히 의료기기 해킹의 경우 단순한 개인정보뿐만 아니라 환자의 민감한 질병 정보와 관련되어 있기 때문에 수집된 정보의 경우 블랙마켓에서 고가로 거래될 가능성이 있음을 강조하였다. 이에 본 논문에서는 스마트 의료 보안과 관련된 국내외 가이드라인을 비교 분석하고 유사한 금융 산업의 보안과도 비교 분석하여 정책적 시사점을 도출하였다.

Ignacio(2021)는 항만의 디지털 변화로 인하여 발생하는 새로운 사이버 보안 위험을 도출하고자 하였다. 항만산업에서 사이버 보안과 관련된 관심은 증가하고 있으나 여전히 항만 안전 및 항만의 활성화와 같이 타 분야에 비하여 연구가 미비하다고 언급하였다. 이에 본 연구는 항만에서 발생하는 사이버 위험에 대하여 보다 객관적인 시각에서 평가하고 사이버 위협에 대한 피해를 완화하기 위한 방법론 개발, 구체적인 대응책인 경보 시스템 및 사이버 사고 대응 정책 수립 등을 제시하였다. 또한, 위험 평가를 위한 새로운 조직 프레임워크 구축의 필요성을 강조하였다. 또한 국제적인 협력과 네트워크 구축이 향후 항만 및 터미널 안전성 강화에 중요한 역할로 작용할 것임을 언급하였다.

Chowdhury and Gkioulous(2021)은 2000년 이후 사이버 보안의 교육유형 및 수준과 관련한 문헌조사를 통하여 중요 인프라 보호를 위한 주요 성과 지표를 수립하고자 하였다. 분석결과 실제 경험 공유, 실제 사용 기술 개발 등 현실적인 솔루션이 다른 교육의 유형보다 우선순위가 높게 나타났다. 이에 본 연구는 지속적인 사이버 보안 교육의 발전 및 제공을 위하여 관련 연구가 수행되어야하며 보다 다양한 방면에서의 사이버 훈련 및 교육 체계가 수립되어야함을 강조하였다.

Ferda et al.(2022)는 의료분야에서의 사이버 보안과 관련하여 연구를 진행하였다. 본 논문은 COVID-19 의 유행으로 인하여 건강 관련 기관을 중심으로 사이버 보안 범죄가 증가되고 있음을 확인하였다. 이에 의료 전문가, IT 전문가의 평가를 통한 두 가지 IT 구성을 설정으로 한 사례 연구를 제시하였으며, 분석 결과 64가지의 다양한 보안 제어가 병원 시스템의 내·외부 공격에서 발생할 가능성이 있는 70가지 취약점과 연결되어있음을 도출하였다. 또한 Microsoft의 STRIDE 범주에 기반하여 새로운 시각화 방법을 포함하고 있어 취약점 및 하위 범주를 관찰할 수 있다는 점에서 그 의미가 있다.

Kim et al.(2022)는 현재 중소기업 및 제조업을 중심으로 지속적인 해킹 범죄가 일어나고 있으나 여전히 국내 사이버 보안과 관련된 낮은 인식을 문제점으로 언급하였다. 이에 본 연구에서는 국내·외에서 발생한 사이버 보안 사고 및 피해 사례에 대하여 실태조사를 실시하였다. 분석결과 해킹과 같은 사이버 침해를 받은 기업은 점차 증가하고 있으나 이 중 96.7%의 기업이 다소 소극적인 태도를 취하고 있음을 확인하였다. 이후 도출된 연구결과를 바탕으로 향후 사이버 보안에 대하여 중소기업의 사이버 보안에 대한 인식 및 역량 강화를 강조하였으며 정부의 적극적인 정책적인 방향성을 제시하였다.

Kim et al.(2023)는 4차 산업혁명, COVID - 19 등 외부적인 변화에 대한 영향으로 여러 산업에서 디지털 전환이 가속화되면서 이에 따라 소프트웨어 공급망 해킹 피해가 증가하고 있다고 언급하였다. 특히 공급망 해킹이 발생할 경우, 단순한 한 부분의 단순 해킹뿐 아니라 더 넓은 시각에서 살펴보면 대규모 해킹으로까지 확산 가능성이 있다고 언급했다. 이에 본 논문은 주요 공급망 피해사례를 면밀하게 분석하여 주요 보안 문제를 파악하였다. 또한 국내 보안정책에 대한 시사점을 도출하기 위하여 주요 국가의 보안 법제 및 표준을 비교 분석을 진행하였다. 이후 분석 결과를 바탕으로 법적 개선, 국가 보안 표준 및 평가체계에 대한 정책적 개선방안을 제안하였다. 선행연구를 바탕으로 정리한 사이버 보안 강화 요인은 다음과 같다.

Seo(2023)은 지진과 태풍과 같은 자연적 요인, 노동자 파업과 같은 인위적 요인, 항만 보안 피해 등이 항만의 안정성에 영향을 미친다고 언급하였다. 이에 본 연구는 각 위험요인별 대응방안을 도출하였다. 특히 항만의 경우 자국산 설비 증진, 선사의 경우 선박자체의 보안을 위한 대응책 또한 강구되어야 한다고 언급하였다.

Table 1 Summary of prior research

Factor		Items	Reference
Legal and Institutional	A1	Legal Framework for Security Management	Song(2013), Lee(2020)
	A2	Establising a Cyber Threat Response System	Song(2013), Oh(2014)
	A3	Formulating Specific Regulations and Strategic Approaches	Yoon et al.(2015), Lee(2020)
	A4	Establishing Security Standards for Cyber Supply Chains	Kim et al.(2022), Kim et al.(2023)
Education and Human resource Development	B1	Cyber security Training for Existing Personnel	Song(2013)
	B2	Training of Cyber security Professionals	Song(2013), Lee(2019)
	B3	Building a Cyber Training System	Chowdhury and Gkioulous(2021)
	B4	Enhancing Security Awareness and Promoting a Security Culture	Song(2013), Yoon et al.(2015)
Network Building and Collaboration	C1	Establishing Domestic and International Networking	Chalermpong(2021), Ignacio(2021)
	C2	Collaboration Among Stakeholders	Jung(2018), Kim et al.(2022)
	C3	Conducting Joint Response Training	Lee(2019)
	C4	Establising a Threat Information Sharing System	Song(2013), Yoon et al.(2015)
Organizational and Policy Support	D1	Expanding Cyber crime Response Units	Song(2013), Hong(2019)
	D2	Developing and Adjusting Organizational Frameworks	Ignacio(2021)
	D3	Active Investment and Budget Increase	Kim et al.(2022)
	D4	Ongoing Formulation of Cyber security-Related Policies	Lee(2020), Kim et al.(2022)

2.2.3 선행연구와의 차별성

최근 적극적인 4차 산업 기술 도입에 따라 항만은 스마트 항만, 자동화 항만 등 보다 디지털 기술을 통한 새로운 항만의 형태로 나아가고 있다. 앞서 진행된 사이버 보안과 관련된 선행연구를 고찰한 결과 해외의 경우 지속적으로 항만 및 터미널의 사이버 보안의 문제점과 개선방안 도출과 관련된 연구가 진행되고 있다. 그러나 국내의 경우 대부분 의료기기, 금융, 선박, 기업 등의 분야에서 사이버 보안과 관련된 연구가 진행되고 있으며 정작 국가적 중요도가 높은 항만의 경우 사이버 보안에 대한 연구가 전무한 실정이다. 따라서 항만의 디지털화가 활발하게 나타나는 시점에서, 국내 컨테이너 터미널의 사이버 보안을 위한 분석을 통한 컨테이너 터미널의 사이버 보안 위협 대응 방안을 모색할 필요가 있다고 판단하였다

이에 본 연구는 세계적인 컨테이너 항만인 부산항을 중심으로 사이버 보안 강화를 위한 요인을 도출하였으며 이후 안전성, 신뢰성, 성과 및 만족도 향상에 대한 다중회귀 분석을 실시하였다는 점에서 다는 점에서 차별성을 지닌다. 분석의 경우 부산항 컨테이너 이해관계자를 대상으로 진행하였으며 도출된 결과를 통하여 부산항 컨테이너 터미널이 사이버 보안을 보다 효과적으로 대응하고 강화하기 위한 요인을 도출하였다. 본 연구의 경우 부산항 컨테이너 항만의 사이버 공격 대응 및 강화를 위한 기초 연구로 의의를 지닌다.

3. 실증분석

3.1 조사 설계

3.1.1 설문조사 개요 및 응답자 현황

부산항 컨테이너 터미널 사이버 보안 강화를 위한 요인분석을 진행하기 위하여 온라인 및 대면 설문조사를 실시하였다. 설문 대상의 경우 대학 및 연구원 종사자, 터미널 운영업체 종사자, 항만공사 및 관련 공기업 종사자 등 부산항 컨테이너 터미널 이해관계자로 설정하였다. 설문조사의 경우 2023. 09. 07. - 2023. 09. 27. 까지 21일간 진행되었다. 수집된 설문지는 총 98부였으나 그 중 중복 응답 2부와 응답이 불성실한 6부를 제외하여 최종적으로 90부의 응답 설문을 바탕으로 본 분석을 실시하였다.

설문 응답자와 관련된 일반 현황은 다음과 같다. 응답자의 근무연수의 경우 10년 이상이 36명(40.00%)로 가장 높게 나타났으며 다음으로 1-3년 20명(22.22%), 5-10년 15명(16.67%), 3-5년 13명 (14.44%), 1년 이하 6명(6.67%)로 나타났다. 또한 응답자의 현재 근무 업종의 경우 터미널 운영업체 33명(36.67%)으로 가장 많은 응답자가 터미널 운영업체에 종사한 것을 확인하였다. 다음으로는 해운기업 및 선사의 경우 24명

(26.67%), 대학 및 연구원은 18명(20.00%), 항만공사 및 관련 공기업 15명(16.67%) 순으로 나타났다.

3.1.2 설문조사 구성

본 분석에 사용된 설문지에 사용된 부산항 컨테이너 터미널 사이버 보안 강화를 위한 요인의 경우 앞서 살펴본 선행연구를 바탕으로 각 요인 도출 후 각 요인의 특성을 고려하여 그룹화하였다. 법·제도적, 교육 및 인력 양성, 네트워크 구축 및 협력, 조직 및 정책 지원 그룹으로 구성되었다. 법·제도적 요인의 경우 보안 관리체계 법적 정비, 사이버 위협 대응 체계 구축, 구체적인 규제 및 전략방안 수립, 사이버 공급망의 보안 표준 제정 등 총 4가지 요소로 구성하였다. 교육 및 인력 양성의 경우 기존 인력 사이버 보안 교육, 사이버 보안 전문 인력 양성, 사이버 훈련 체계 구축, 보안 인식 제고 및 보안 문화 확산 등 총 4가지 요소로 구성하였다. 네트워크 구축 및 협력의 경우 국·내외 상호 네트워크 구축, 이해관계자 간 협력, 합동 대응 훈련 시행, 위협정보 공유체계 구축 등 총 4가지 요소로 구성하였다. 마지막으로 조직 및 정책 지원의 경우 사이버 범죄 전담 대응 기구 확대, 조직적 프레임워크 개발 및 조정, 적극적인 투자 및 예산 증대, 지속적인 사이버 보안 관련 정책 수립 등 총 4가지 요소로 구성하였다. 최종적으로 부산항 컨테이너 터미널 사이버 보안 강화를 위한 요인분석 연구와 관련된 설문지의 경우 강화 요인 16가지를 구성하여 분석을 진행하였다. 진행된 설문조사의 경우 설문지 회수의 용이성 및 응답 편의성을 위하여 Likert 5점 척도로 구성하였다. 설문지에 제시된 세부 요인은 Table 2과 같다.

Table 2 Summary of survey

Factor		Items
Legal and Institutional	A1	Legal Framework for Security Management
	A2	Establising a Cyber Threat Response System
	A3	Formulating Specific Regulations and Strategic Approaches
	A4	Establishing Security Standards for Cyber Supply Chains
Education and Human resource Development	B1	Cyber security Training for Existing Personnel
	B2	Training of Cyber security Professionals
	B3	Building a Cyber Training System
	B4	Enhancing Security Awareness and Promoting a Security Culture
Network Building and Collaboration	C1	Establishing Domestic and International Networking
	C2	Collaboration Among Stakeholders
	C3	Conducting Joint Response Training
	C4	Establishing a Threat Information Sharing System
Organizational and Policy Support	D1	Expanding Cyber crime Response Units
	D2	Developing and Adjusting Organizational Frameworks
	D3	Active Investment and Budget Increase
	D4	Ongoing Formulation of Cyber security-Related Policies

3.2 탐색적 요인분석

요인분석(Factor Analysis)은 각 변수 사이에 나타나는 상호 연관성을 분석하고 공통 정보를 대표 요인으로 추출하는 분석기법이다. 요인분석은 탐색적 요인분석과 확인적 요인분석으로 구분될 수 있다. 요인분석은 실시하는 목적에 따라서 탐색적 요인분석(Exploratory facotr analysis)과 확인적 요인분석(Confirmatory factor analysis)으로 분류될 수 있다. 탐색적 요인분석은 변수 간 구조를 파악하고 통계적 효율성을 높이기 위하여 대표 변수를 도출하는 방법이다. 이는 변수와 요인 간의 관계가 이론적으로 정립되지 않거나 논리적으로 체계화되지 않은 상태에서 주로 활용되며 SPSS, SAS 등의 프로그램을 통해 수행되는 기법이다(최창호 외 1인, 2017). 본 분석의 경우 요인과 요인의 수가 정형화되지 않고 기본 구조가 확립되지 않아 새로운 이론을 체계화하고 연구의 방향을 파악하기 위해서 탐색적 요인분석을 진행하였다. 신뢰도 분석의 경우 요인분석 진행 시 연구 대상을 반복 측정을 가정하였을 때 동일한 값을 도출하는 가능성을 확인하는 분석이다.

본 설문에 사용된 변수의 경우 체계화되어있지 않으며 항만 및 컨테이너 터미널의 사이버 보안을 강화할 수 있는 요인으로 판단되는 변수이다. 따라서 탐색적 요인분석을 통하여 각 변수를 적합하게 재구분할 필요가 있다고 판단하였다. 탐색적 요인분석과 신뢰도 분석을 위하여 SPSS 23.0을 활용하여 분석을 진행하였다. 분석 방법의 경우 변수들의 상관관계를 이용하여 유사한 변수끼리 묶는 배리맥스 직각회전 요인분석방식으로 선정하였다. 고유값의 경우 1을 기준으로 하도록 설정하였다.

탐색적 요인분석을 실시하기 전 KMO 척도와 Bartlett 구형성 검정을 통하여 수집된 표본의 적합도를 검증하였다. 통상적으로 KMO의 값이 0.5 이상이면 요인분석을 수행함에 있어 적합한 자료라고 할 수 있으며 Bartlett 검정의 경우 유의확률이 0.05 이하일 경우 적합하다고 판단할 수 있다(Nam, 2022). 본 연구의 검정 분석 결과 KMO 값은 0.884, Bartlett 구형성 검정 결과 유의확률이 0.00으로 0.05 이하로 나타났다. 따라서

요인분석의 사용이 적합하다고 판단하였다. 이후 탐색적 요인분석을 실시하였다. 탐색적 요인분석에서 나타나는 요인적재량은 통상적으로 요인적재량이 0.3 이상이면 유의적이라고 판단하나 보수적인 견해에서는 0.5 이상으로 판단하고 있다. 이에 본 연구에서는 요인적재량 0.5 이상을 기준으로 선정하여 탐색적 요인분석을 진행하였다. 분석 결과 모든 요인의 요인적재값이 0.5 이상으로 매우 유의한 결과 값으로 분석되었다.

최종적으로 16개의 변수를 3개의 요인으로 분류되었으며 이 이후 신뢰성 분석을 실시하였다. 신뢰성 값을 해석하는 기준은 학자마다 상이하나 일반적으로 사회과학 분야에서는 0.6 이상이면 신뢰도 값이 있다고 본다. 분석 결과 본 연구에서 Cronbach α(알파)의 값이 요인 1은 0.849, 요인 2는 0.843, 요인 0.798로 매우 높은 신뢰성을 확보하였다. 분석 결과는 Table 3과 같다. 이후 탐색적 요인분석을 실시하였다. 탐색적 요인분석에서 나타나는 요인적재량은 통상적으로 요인적재량이 0.3 이상이면 유의적이라고 판단하나 보수적인 견해에서는 0.5 이상으로 판단하고 있다.

이에 본 연구에서는 요인적재량 0.5 이상을 기준으로 선정하여 탐색적 요인분석을 진행하였다. 분석 결과 모든 요인의 요인 적재값이 0.5 이상으로 매우 유의한 결과값으로 분석되었다.

최종적으로 16개의 변수를 3개의 요인으로 분류되었다. 분석 이후 신뢰성 분석을 실시하였다. 신뢰성 값을 해석하는 기준은 학자마다 상이하나 일반적으로 사회과학 분야에서는 0.6 이상이면 신뢰도 값이 있다고 본다. 분석 결과 본 연구에서 Cronbach α(알파)의 값이 요인 1은 0.849, 요인 2는 0.843, 요인 0.798로 매우 높은 신뢰성을 확보하였다.

분석 결과는 Table 3과 같다. 분류된 변수를 고려한 최종 요인명칭은 다음과 같다. 요인 1은 D2 (조직적 프레임워크 개발 및 조정), D4 (지속적인 사이버 보안 관련 정책 수립), C2 (이해관계자 간 협력), D3 (적극적인 투자 및 예산 증대), C1 (국·내외 상호 네트워크 구축) 구성되었다. 이에 본 요인을 네트워크 구축 및 정책 지원 요인으로 정의하였다. 요인 2의 경우 A4 (사이버 공급망의 보안표준 제정), B3 (사이버 훈련 체계 구축), B1 (기존 인력 사이버 보안 교육), C3 (합동 대응 훈련 시행), B2 (사이버 보안 전문 인력 양성) 로 구성되었다. 이에 본 요인을 교육 표준화및 인력 양성으로 정의하였다. 요인 3의 경우 A1 (보안 관리체계 법적 정비), A3 (구체적인 규제 및 전략방안 수립), B4 (보안 인식 제고 및 보안 문화 확산), C4 (사이버 위협정보 공유체계 구축), A2 (사이버 위협 대응 체계 구축) 로 구성되었다. 이에 본 요인을 법·제도적 요인으로 정의하였다.

Table 3 Result of exploratory factor analysis and reliability analysis

Element			Factor			Cronbach α
Before analysis	After analysis		1	2	3	
D2	Network Establishment and Policy Support Factors	A1	0.753			0.849
D4		A2	0.749			
C2		A3	0.708			
D1		A4	0.647			
D3		A5	0.632			
C1		A6	0.563			
A4	Education Standardization and Workforce Development	B1		0.780		0.843
B3		B2		0.738		
B1		B3		0.627		
C3		B4		0.594		
B2		B5		0.593		
A1	Legal and Institutional	C1			0.785	0.798
A3		C2			0.676	
B4		C3			0.604	
C4		C4			0.587	
A2		C5			0.504	
KMO 0.859 Bartlett 0.000 Survey 90						

3.3 다중회귀분석

회귀분석이란 독립변수가 종속변수와 독립변수 간 연관성을 파악하고 이를 선형모형으로 산출하는 방법이다. 본 연구에서는 다중회귀분석을 통하여 부산항 컨테이너 터미널 변화에 미치는 사이버 보안 강화 요인을 도출하고자 하였다. 본 분석에서는 각 요인이 종속변수에 미치는 영향을 자세하게 분석하기 위하여 16가지 요인을 독립변수로 선정하였으며 종속변수는, 컨테이너 터미널의 안전성 확보 및 강화에 영향, 컨테이너 터미널의 신뢰성 확보 및 강화에 영향, 컨테이너 터미널의 성과 및 만족도 향상으로 설정하였다.

3.3.1 부산항 컨테이너 터미널의 안전성 확보 및 강화에 대한 다중회귀분석

부산항 컨테이너 터미널의 안전성 확보 및 강화에 대한 다중회귀분석을 진행한 결과 A2 (지속적인 사이버 보안 관련 정책 수립), C5 (사이버위협 대응 체계 구축) 변수가 $|t| > 1.96$ 이상, 유의확률 0.05 이하로 채택되었다. 이는 사이버위협 대응 체계 구축 요인과 지속적인 사이버 보안 관련 정책 수립 요인이 컨테이너 터미널 안전성 확보 및 강화에 영향을 미치는 것을 의미한다. 또한 각 요인의 표준화 계수를 살펴보면 각각 0.292, 0.307으로 두 요인 모두 정(+)의 방향인 것을 확인할 수 있다. 이는 부산항 컨테이너 사이버 보안을 위한 적극적인 사이버 위협 대응 체계 구축과 지속적인 사이버 보안 관련 정책 수립을 통하여 컨테이너 터미널의 안전성 확보 및 강화에 긍정적 영향을 미치는 것으로 해석된다. 또한 표준화 계수를 통하여 사이버 위협 대응 체계 구축이 터미널의 안전성 확보 및 강화에 비교적 더 중요한 요인임을 확인할 수 있다. 분석 결과는 Table 4과 같다.

3.3.2 부산항 컨테이너 터미널의 신뢰성 확보 및 강화에 대한 다중회귀분석

부산항 컨테이너 터미널의 신뢰성 확보 및 강화에 대한 다중회귀분석 결과 A3 (이해관계자 간 협력), C4 (위협정보 공유체계 구축) 변수가 $|t| > 1.96$ 이상, 유의확률 0.05 이하로 채택되었다. 이는 이해관계자 간 협력 요인과 위협정보 공유체계 구축이 컨테이너 터미널 신뢰성 확보 및 강화에 영향을 미치는 것을 의미한다. 또한 각 요인의 표준화 계수를 살펴보면 각각 0.295, 0.289로 두 요인 모두 정(+)의 방향인 것을 확인할 수 있다. 이는 부산항 컨테이너 사이버 보안을 위한 적극적인 이해관계자 간 협력과 체계적인 위협정보 공유체계 구축을 통하여 컨테이너 터미널의 신뢰성 확보 및 강화에 긍정적 영향을 미치는 것으로 해석된다. 또한 표준화 계수를 통하여 이해관계자 간 협력이 터미널의 신뢰성 확보 및 강화에 비교적 더 중요한 요인임을 확인할 수 있다. 분석 결과는 Table 5과 같다.

3.3.3 부산항 컨테이너 터미널의 성과 및 만족도 향상에 대한 다중회귀분석

부산항 컨테이너 터미널의 성과 및 만족도 향상에 대한 다중회귀분석 결과 A4 (사이버 범죄 전담 대응 기구 확대), C3 (보안 인식 제고 및 보안 문화 확산), 변수가 $|t| > 1.96$ 이상, 유의확률 0.05 이하로 채택되었다. 이는 보안 인식 제고 및 보안 문화 확산과 사이버 범죄 전담 대응 기구 확대 요인이 컨테이너 터미널 성과 및 만족도 향상에 영향을 미치는 것을 의미한다.

Table 4 The results of multiple regression analysis for ensuring and enhancing safety at Busan Port container terminals

Model		Unstandardized		Standardize	T-value	P-value	Tolerance	VIF
		B	Std. Error	Beta				
Network Establishment and Policy Support Factors	A1	.159	.103	.182	1.536	.129	.436	2.291
	A2	.242	.098	.292	2.482	.015	.440	2.273
	A3	.091	.123	.091	.739	.462	.401	2.492
	A4	.027	.107	.034	.259	.799	.350	2.857
	A5	-.091	.094	-.105	-.969	.336	.524	1.908
	A6	-.042	.088	-.056	-.477	.635	.450	2.222
Education Standardization and Workforce Development	B1	-.027	.105	-.031	-.258	.797	.422	2.368
	B2	-.073	.117	-.088	-.628	.532	.311	3.211
	B3	.050	.090	.057	.556	.580	.574	1.741
	B4	.035	.091	.045	.385	.701	.438	2.285
	B5	-.088	.112	-.103	-.783	.436	.355	2.815
Legal and Institutional	C1	.124	.104	.125	1.194	.236	.554	1.804
	C2	-.221	.115	-.228	-1.918	.059	.430	2.326
	C3	.128	.109	.148	1.174	.244	.386	2.589
	C4	.086	.101	.205	1.838	.070	.490	2.039
	C5	.302	.100	.307	3.015	.004	.590	1.695
Constant = 0.745, R^2= 0.555, Adj R^2= 0.457, F=5.687, P=0.00, Durbin-Watson : 1.884								

Table 5 The results of multiple regression analysis for ensuring and enhancing safety at Busan Port container terminals

Model		Unstandardized		Standardize	T-value	P-value	Tolerance	VIF
		B	Std. Error	Beta				
Network Establishment and Policy Support Factors	A1	-.020	.109	-.022	-.186	.853	.436	2.291
	A2	.169	.103	.195	1.633	.107	.440	2.273
	A3	.307	.130	.295	2.353	.021	.401	2.492
	A4	.169	.113	.202	1.504	.137	.350	2.857
	A5	-.100	.100	-.110	-1.000	.321	.524	1.908
	A6	.015	.093	.019	.162	.872	.450	2.222
Education Standardization and Workforce Development	B1	-.175	.111	-.193	-1.582	.118	.422	2.368
	B2	-.059	.124	-.067	-.473	.637	.311	3.211
	B3	.070	.096	.077	.734	.465	.574	1.741
	B4	-.060	.096	-.075	-.625	.534	.438	2.285
	B5	.037	.118	.042	.317	.752	.355	2.815
Legal and Institutional	C1	.040	.109	.039	.368	.714	.554	1.804
	C2	.125	.122	.124	1.022	.310	.430	2.326
	C3	.069	.115	.077	.602	.549	.386	2.589
	C4	.273	.107	.289	2.547	.013	.490	2.039
	C5	-.020	.106	-.019	-.185	.854	.590	1.695
Constant = 0.735, R^2= 0.540, Adj R^2= 0.439, F=5.356, P=0.00, Durbin-Watson : 2.292								

또한 각 요인의 표준화 계수를 살펴보면 각각 0.288, 0.320으로 두 요인 모두 정(+)의 방향인 것을 확인할 수 있다. 이는 부산항 컨테이너 사이버 보안을 위하여 적극적인 관계자들의 보안 인식 제고 및 문화 확산과 사이버 범죄 전담 대응 기구 확대를 통하여 컨테이너 터미널의 성과 및 만족도 향상에 긍정적 영향을 미치는 것으로 해석된다. 또한 표준화 계수를 통하여 보안 인식 제고 및 보안 문화 확산이 터미널의 성과 및 만족도 향상에 비교적 더 중요한 요인임을 확인할 수 있다. 분석 결과는 Table 6과 같다.

4. 결 론

4.1 연구 결과 및 시사점

항만은 점차 항만 운영의 효율성 및 생산성 향상과 운영비 절감 등을 위해 보다 적극적인 4차 산업 기술 활용을 추진하고 있다. 그러나 이러한 항만의 디지털화, 스마트화가 진행됨과 동시에 항만의 기술 의존도가 높아지고 있으며 이는 항만 내 사이버 보안 위험과 같은 새로운 위협 요인을 초래하였다. 항만의 경우 현재 국가보안시설이며 최근 항만, 공항 등의 국

Table 6 The results of multiple regression analysis for ensuring and enhancing safety at Busan Port container terminals

Model		Unstandardized		Standardize	T-value	P-value	Tolerance	VIF
		B	Std. Error	Beta				
Network Establishment and Policy Support Factors	A1	.048	.132	.045	.362	.718	.436	2.291
	A2	.179	.124	.178	1.439	.155	.440	2.273
	A3	-.028	.157	-.023	-.181	.857	.401	2.492
	A4	.282	.136	.288	2.080	.041	.350	2.857
	A5	-.047	.120	-.044	-.388	.699	.524	1.908
	A6	.075	.112	.082	.670	.505	.450	2.222
Education Standardization and Workforce Development	B1	.095	.133	.090	.713	.478	.422	2.368
	B2	-.158	.149	-.156	-1.061	.292	.311	3.211
	B3	.011	.115	.010	.093	.923	.574	1.741
	B4	.122	.116	.130	1.052	.296	.438	2.285
	B5	-.012	.142	-.012	-.086	.932	.355	2.815
Legal and Institutional	C1	-.013	.132	-.011	-.099	.921	.554	1.804
	C2	-.014	.147	-.012	-.094	.925	.430	2.326
	C3	.338	.139	.320	2.431	.017	.386	2.589
	C4	.062	.129	.056	0.478	.634	.490	2.039
	C5	.008	.128	.006	0.059	.953	.590	1.695
Constant = 0.714, R^2= 0.510, Adj R^2= 0.403, F=4.758, P=0.00, Durbin-Watson : 1.838								

가 보안 시설의 경우 사이버 공격의 주요 대상으로 나타나고 있다. 이러한 변화 흐름을 살펴보았을 때 향후 항만을 대상으로 발생되는 사이버 보안 사고는 지속적으로 증가될 가능성이 높다. 이에 본 연구는 국내 대표 항만인 부산항을 연구 대상으로 선정하였으며 항만 내에서 가장 자동화, 디지털화가 활발하게 나타나고 있는 컨테이너 터미널을 대상으로 분석을 진행하였다. 요인분석 및 다중회귀분석을 바탕으로 도출한 결과는 다음과 같다.

첫째, 부산항 컨테이너 터미널 사이버 보안 강화를 위한 탐색적 요인분석 및 신뢰도 분석 결과 네트워크 구축 및 정책 지원요인, 교육 체계 표준화 및 인력 양성 요인, 법·제도적 요인 등 세 가지 요인이 도출되었다.

둘째, 부산항 컨테이너 터미널의 안전성 확보 및 강화에 대한 다중회귀분석 결과 지속적인 사이버 보안 관련 정책 수립 요인과 사이버 위협 대응 체계 구축 요인이 통계적으로 정(+)의 방향으로 유의하게 나타났다. 이를 통하여 지속적인 사이버 보안 관련 정책 수립과 사이버 위협 대응 체계 구축이 강화될수록 부산항 컨테이너 터미널의 안전성 확보가 향상됨을 확인하였다. 최근 사이버 보안과 관련된 정책을 살펴보면 빠르게 발전하는 사이버 보안 공격에 비하여 이를 관리 및 대응할 수 있는 정책적인 대응 방안은 여전히 부족한 것을 확인할 수 있다. 또한 사이버 보안 위협 대응 체계는 국가 안보실을 포함하여 기업, 민간의 경우 과학기술정보통신부 등 영역별로 대응하고 있다. 따라서 현재 사이버 공격에 대하여 정보 공유가 제대로 이루어지지 않고 있으며 종합적인 분석 및 대응에 한계를 지닌다. 따라서 컨테이너 터미널 안전성 확보 및 강화를 위해서는 항만의 특성을 고려하여 구체적인 사이버 보안 정책을 수립해야하며, 일원화된 사이버 위협 대응 체계를 구축할 필요성이 있다.

셋째, 부산항 컨테이너 터미널의 신뢰성 확보 및 강화에 대한 다중회귀분석 결과 이해관계자 간 협력 요인과 위협정보 공유체계 구축 요인이 통계적으로 정(+)의 방향으로 유의하게 나타났다. 이를 통하여 이해관계자 간 협력과 위협정보 공유체계 구축이 강화될수록 부산항 컨테이너 터미널의 신뢰성 확보가 향상됨을 확인하였다. 사이버 공격은 다양한 조직과 시스템을 대상으로 하고 있으며 이러한 위험 대응 및 위협정보를 각 국가 및 기업이 독자적으로 수집하는 것은 비효율적으로 생각된다. 따라서 보다 적극적인 이해관계자 간 협력과 위협정보 공유체계 구축을 통하여 실시간 대응 능력 향상과 효율적인 보안 대책 수립을 바탕으로 전체적인 사이버 안전성을 향상시킬 필요가 있다. 나아가 이해관계자들의 협력과 정보 공유는 다양한 시각으로 사이버 공격을 분석할 수 있기에 향후 발생될 수 있는 사이버 공격에 대하여 다양한 방식으로 대응이 가능할 것으로 기대할 수 있다.

넷째, 부산항 컨테이너 터미널의 성과 및 만족도 향상에 대한 다중회귀분석 결과 사이버 범죄 전담 대응 기구 확대 요인과 보안 인식 제고 및 보안 문화 확산 요인이 통계적으로 정(+)의 방향으로 유의하게 나타났다. 이를 통하여 사이버 범죄 전담 대응 기구 확대와 보안 인식 제고 및 보안 문화가 강화될수록 부산항 컨테이너 터미널의 성과 및 만족도가 향상됨을 확인하였다. 컨테이너 터미널의 경우 터미널 운영 시스템 뿐 아니라 다양한 화물 및 관계자들의 데이터가 관리되는 공간이다. 이러한 터미널이 사이버 공격을 받는다면 시스템 마비, 데이터 유출 및 훼손으로 인하여 물리적 보안 문제까지 확산 될 수 있다. 화물의 손상은 항만 및 컨테이너 터미널의 성과 및 만족도에 치명적인 악영향을 미친다. 따라서 사이버 전담 대응 기구를 확대하여 공격에 대한 신속하고 효과적인 대응 및 화물 등 터미널 내에서 생성되는 데이터에 대한 안전성을 확보할 필요가 있다. 또한 보안 인식 제고 및 보안 문화 확산을 통하여 이해관계자들의 사이버 위협 대응 능력을 강화하고 안전한 작업 환경 조성을 통하여 결과적으로 컨테이너 터미널의 만족도를 향상시킬 수 있을 것이다.

마지막으로 다중회귀분석 결과를 살펴보면 부산항 컨테이너 터미널의 안전성 확보 및 강화, 신뢰성 확보 및 강화, 성과 및 만족도 향상을 위한 요인 중 교육 표준화 및 인력 양성에 해당하는 요인이 포함되지 않은 것을 확인할 수 있다. 현재 사이버 보안과 관련된 교육 및 훈련 양성의 경우 대부분 기업 내에서 자체적으로 이루어지는 것이 아닌 전문 업체에 위탁하여 진행되고 있다. 따라서 부산항 컨테이너 터미널의 이해관계자들은 교육 및 인력양성의 경우 타 요인에 비하여 부산항 발전에 간접적 요인으로 인식하고 있는 것으로 판단된다.

4.2 연구의 한계점 및 향후 연구방향

최근 항만 및 컨테이너 터미널 내에서 발생 사이버 보안 공격 동향을 통하여 모든 항만이 공격 대상이 될 수 있음을 확인할 수 있다. 그러나 본 연구는 연구 대상을 부산항 컨테이너 터미널로 한정하여 분석을 진행했다는 점에서 연구의 한계점을 지닌다.

따라서 향후 연구에서는 인천항, 평택항, 울산항 등 분석 대상을 국내 항만으로 확장하여 연구를 진행할 필요성이 있다. 또한 본 연구의 경우 대부분의 요인들이 정책적 요인으로 구성되어있다. 따라서 향후 연구에서는 강화 방안을 정책적 요인 뿐 아니라 4차 산업 기술을 활용한 방안까지 고려하여 연구를 진행할 필요가 있다고 판단된다.

References

[1] Bae, S. K.(2015), “Examen de la politique de Cybersécurité au Japon – Focaliser sur l’établissement et la révision de la loi fondamentale sur la Cybersécurité –”, HUFS Law Review, Vol. 42, No. 2, pp. 141-165.

[2] Chalermpong, S.(2021), “Port Cyber security and threat : A structural modal for prevention and policy development”, The Asian Journal of Shipping and

Logistics, Vol. 37, Vol. 37, pp. 20-36.
[3] Ferda, Ö. S. et al.(2022), "Decision support for healthcard Cyber security", Computers & Security, Vol 122.
[4] Gunes, B. et al.(2021), "Cyber security risk assessment for seaports: A case study of a container port", Computers & Security, Vol. 103.
[5] Hong, J. H.(2019), "Research on the Necessity of Cyber Security Control Tower", Law Review (korlaw), Vol. 19, Vol. 1, pp. 235-254.
[6] Jung, N. Y.(2018), "A Study on Strengthening Cybersecurity for Critical Infrastructure of Energy Sector", Sangmyung University, Graduate School of Management, M.A Dissertation.
[7] Kang, D. Y.(2019), "Factors Affecting the Security Ability of Port Logistics Organization Members", Journal of Korean Navigation and Port Reserch, Vol. 43, No. 3, pp. 179-185.
[8] Kang, M. G. and Kim, H. W.(2019), "A Study on the Relative Importance of Evaluation Factors for Improvement of Port Security", Journal of Korean Navigation and Port Reserch, Vol. 43, No. 1, pp. 49-56.
[9] Kim, J. M., Han H. M. and Kim. J. H.(2022), "Cyber Security Policies for Small and Medium-sized Enterprises (SMEs): A Case Study on the Cyber Security Breaches in Manufacturing SMEs in Korea", The e-Business Studies (Tebs), Vol. 23, No. 3, pp. 41-63.
[10] Kim, J. M. et al.(2023), "A Study on Cyber Security Policy for S/W Supply Chain Security in Korea", The Journal of Society for e-Business Studies, Vol. 28, No. 1, pp. 29-53.
[11] Lee, C. K.(2019), "A Study of cyber financial security measures in the UK" Journal of Payment and Settlement, Vol. 11, No. 1, pp. 195-214.
[12] Lee, E. S. and Park, S. H.(2021), "A Legislative Study for strengthening of Ship Cyber Security", MARITIME LAW REVIEW, Vol. 33, No. 2, pp. 227-254.
[13] Lee, H. W. and Kim, J. B.(2014), "An Empirical Investigation on the Effect of LogisticsSecurity in Import and Export Risk Management", Journal of Korean Navigation and Port Reserch, Vol. 38, No. 3, pp. 317-325.
[14] Lee, J. E.(2020), "A research on Cyber security policy improvement for smart healthcare industry", Soongsil University, Graduate School of Information Science, M.A Dissertation.
[15] Nabin, C. and Gkioulos, V.(2021), "Cyber security training for critical infrastructure protection: A literature review", Computer Science Review, Vol. 40, No. 3, pp. 179-185.
[16] Nam, J. W. et al.(2022), "A Data Factorization Study for the Application of Digital Twin Technology to Container Port", Journal of Korean Navigation and Port Reserch, Vol. 46, No. 1, pp. 42-56.
[17] Oh, I. S.(2014), "A Legal Study on Enhancing Security Authority's Cyber Security Activities", Hannam Journal of Law&Technology, Vol. 20, No. 3, pp. 41-90.
[18] Penttilä and Olli-Jussi, J.(2016), "Cyber Threats in Maritime Container Terminal Automation Systems", Tampere University of Technology, Graduate School of Computational Electrical Engineering, M.A Dissertation.
[19] Seo, K. W.(2023), "Legal Study on the Various Risks that Threaten Port Function", The Journal of Korea Maritime Law Association, Vol. 45, No. 2, pp. 35-65.
[20] Song, B. H.(2013), "A Countermeasure on Investigation and Security Agency to Change of Cyber Terrorism", Korean terrorism studies Review, Vol. 6, No. 4, pp. 75-92.
[21] Yoon, O. J. et al.(2015), "A Study on Measures for Strengthening Cybersecurity through Analysis of Cyberattack Response", Journal of convergence security, Vol. 15, No. 4, pp. 65-72.
[22] Yoo, Y. J. et al.(2023), "Cybersecurity Development Status and AI-Based Ship Network Security Device Configuration for MASS", Journal of Korean Navigation and Port Reserch, Vol. 47, No. 2, pp. 57-65.

Received 29 November 2023
Revised 14 December 2023
Accepted 20 December 2023