Journal of Korea Port Economic Association
Vol.40, No.1, 2024, pp.1-14.
https://doi.org/10.38121/kpea.2024.3.40.1.1

부산항 컨테이너 터미널 사이버 보안 강화를 위한 우선순위 분석*

하도연** · 김치열*** · 김율성****

Prioritization Analysis for Cyber Security Enhancement at Busan Port Container Terminal

Ha, Do-Yeon · Kim, Chi-Yeol · Kim, Yul-Seong

Abstract

The port industry has been actively adopting Fourth Industrial Revolution technologies, leading to transformations in port infrastructure, such as automated and smart ports. While these changes have improved port efficiency, they have also increased the potential for Cyber Security incidents, including data leaks and disruptions in terminal operations due to ransomware attacks. Recognizing the need to prioritize Cyber Security measures, a study was conducted, focusing on Busan Port's rapidly automating container terminal in South Korea.

The results of the Eisenhower Matrix analysis identified legal and regulatory factors as a top priority in the first quadrant, with educational systems, workforce development, network infrastructure, and policy support in the third quadrant. Subsequently, a Borich Needs Analysis revealed that the highest priority was given to legal improvements in security management systems, while the development of Cyber Security professionals ranked lowest.

This study provides foundational research for enhancing Cyber Security in domestic container terminals and offers valuable insights into their future direction.

Key words: Busan port, Container Terminal, Cyber security, Priority

▷ 논문접수: 2023. 11. 24. ▷ 심사완료: 2023. 12. 18. ▷ 게재확정: 2023. 12. 28.

* 본 논문은 한국해양수산개발원이 후원한 해운항만 디지털 전환에 따른 대응전략 논문 공모전 수상작임을 밝힙니다.
** 한국해양대학교 KMI-KMOU 학연협동과정 석사과정, 제1저자, ehdudl6091@g.kmou.ac.kr
*** 한국해양대학교 해양경영경제학부 교수, 공동저자, cykim@kmou.ac.kr
**** 한국해양대학교 물류시스템학과 교수, 교신저자, logikys@kmou.ac.kr

Ⅰ. 서 론

4차 산업혁명의 기술은 여러 분야에서 활용되고 있으며 특히 해운 및 항만 분야는 적극적으로 신기술을 도입하고 있다. 이에 항만은 점차 자동화 항만, 스마트 항만 등의 모습으로 변화하고 있다. 해외의 경우 로테르담항, LA/LB항, 청도항 등이 완전 자동화 터미널을 운영하고 있으며 국내의 경우 2023년에 국내 최초 완전 자동화 항만인 부산 신항 2-5단계가 개장을 앞두고 있다. 이러한 흐름을 통해 항만의 4차 산업 기술 도입은 더 이상 경쟁 우위를 위한 선택적 사항이 아닌 항만의 지속적인 성장을 위한 필수 요인임을 확인할 수 있다.

항만 운영의 자동화는 작업 프로세스의 무인화를 통한 항만 운영비 절감, 효율성 및 생산성 증대 효과 등 항만 운영의 다양한 긍정적 효과를 나타낸다. 또한 실시간 정보공유, 안전성 증대, 데이터 분석 및 최적화 등을 통하여 항만 이해관계자의 만족도를 향상시킬 수 있다. 그러나 최근 긍정적 변화에 반대되어 항만 내 사이버 위협 가능성이 높아지고 있다. 2023년 EU의 사이버 보안국인 ENISA이 발표한 자료에 따르면 사이버 공격이 점차 항공, 철도, 해양 등 운송 분야 내 발생될 가능성이 향상되고 있음을 확인할 수 있다. 특히 현재 진행되고 있는 러시아-우크라이나 전쟁으로 인하여 운송 부문의 사이버 보안 공격이 증가할 것으로 예상하였다. 실제로 2022년 12월 Lison 항만과 2023년 나고야항만이 사이버 공격으로 인하여 항만 및 컨테이너 터미널 운영이 중단되었다.

이처럼 항만 및 컨테이너 터미널 내 자동화가 가속화됨에 따라 사이버 보안의 공격 또한 점차 증가하고 있다. 항만의 경우 국가보안시설이며 국가 전체의 수출입 관문 역할을 수행하고 있다. 따라서 항만 내에서 발생하는 사이버 보안 문제는 항만 운영 시스템 마비뿐만 아니라 확장된 시각에서 본다면 국가 전체의 경제적 및 안전의 위험에 영향을 미칠 수 있다. 따라서 항만 및 컨테이너 터미널 내에서 발생 될 수 있는 사이버 보안 공격에 대하여 선제적 대응책을 도출하고 활발한 연구가 필요하다고 판단하였다. 해외의 경우 이러한 항만 및 컨테이너 터미널 내 사이버 보안 문제를 인지하고 지속적으로 사이버 보안 강화방안과 관련된 연구가 진행되고 있다. 그러나 국내의 경우 사이버 보안 관련 연구 대상이 대부분 금융, 원자력, 의료 등으로 항만 및 컨테이너 터미널을 대상으로 한 연구는 매우 미비한 실정이다. 이에 국내 항만의 사이버 보안 공격에 선진적으로 대응하기 위하여 강화 요인의 우선순위를 도출하고자 하였다.

본 연구는 국내 대표 항만인 부산항 중 자동화가 빠르게 나타나고 있는 컨테이너 터미널을 대상으로 설정하였다. 분석의 경우 부산항 컨테이너 터미널의 이해관계자를 대상으로 설문조사를 진행하였다. 이후 Microsoft Excel을 활용하여 아이젠하워 매트릭스 분석과 Borich 요구도 분석을 진행하였다. 분석을 통해 도출된 결과를 바탕으로 부산항 컨테이너 터미널이 사이버 보안 강화 요인의 우선순위를 제시하였다. 도출된 연구 결과는 향후 부산항 컨테이너 터미널 사이버 보안 강화 전략 수립 시 활용될 수 있는 기초자료로 활용될 것을 기대한다.

Ⅱ. 항만 및 컨테이너 터미널의 사이버 보안 현황

전 세계적으로 적극적인 4차 산업 기술 도입을 통한 항만의 자동화 변화가 활발하게 나타나고 있다. 그러나 이러한 변화 속에서 항만의 기술 의존도 또한 높아짐에 따라 최근 항만은 사이버 공격의 주요 대상으로 나타났다. 2020년의 6월 이란의 샤히드 라자이 항만은 대규모 사이버 공격을 받았다. 샤히드 라자이 항만의 경우 다량의 물동량을 처리하고 있어 이란 내에서 중요한 역할을 수행하고 있다. 발생된 사이버 공격으로 인하여 해당 항만은 선박 운항, 물

류 관리 시스템 등이 마비되었으며 화물손실 등 물리적 피해가 발생하였다. 본 사례를 통하여 항만 및 컨테이너 터미널의 사이버 보안 공격의 경우 항만 운영의 중단, 물리적인 피해까지 영향을 미칠 수 있음을 확인할 수 있다. 또한 워싱턴에 케네웍 항만의 경우 2020년 11월 랜섬웨어 공격으로 인하여 서버에 대한 접근이 차단되는 사고가 발생하였다. 해당 사고로 인하여 케네웍 항만은 약 일주일가량 항만의 원활한 운영에 어려움을 겪었다. 특히 본 항만의 경우 작은 내륙 항만으로 주요 상업항만보다 규모 및 처리 물동량이 현저하게 적었음에도 불구하고 사이버 범죄의 대상 항만이 되었다. 이를 통하여 사이버 보안 공격 항만의 경우 항만의 위치 및 처리 물동량에 상관없으며 오히려 규모가 작은 항만은 사이버 보안과 관련된 방어 체계가 체계화되지 않았기 때문에 범죄 대상 항만이 될 수 있음을 파악하였다. 일본의 나고야 항만에서는 2023년 7월 랜섬웨어 감염 사고가 발생하였다. 본 사고의 경우 아시아에서 나타나는 최대 규모의 랜섬웨어 사고이며 감염으로 인하여 컨테이너 하역 및 운반을 관리하는 전산 시스템 감염으로 인하여 터미널의 반입·반출 작업이 정지되었다. 해당 사건 이후 일본 정부는 사이버 환경 변화를 인지하였으며 향후 항만 내 사이버 보안 대응 전략 수립 및 체계화를 통한 선진적 방어 체계를 구축하고 있다. 이뿐만 아니라 2011년 앤트워프 악성코드 침투, 2018년 롱비치항 랜섬웨어, 2020년 마르세유 항만 랜섬웨어 감염 등 지속적인 항만의 사이버 공격이 발생하고 있다. 영국 방송공사인 BBC에 따르면 세계적인 항만인 LA항만은 코로나-19 이후 사이버 공격이 약 두 배 증가했음을 언급하였다. 이를 통하여 항만 내 사이버 보안은 급격한 증가추세를 보이고 있으며 발생한 항만 및 컨테이너 터미널 내 사이버 보안 사고 사례를 통해 항만의 크기나 위치에 상관없이 모든 항만에서 사이버 보안사고 가능성이 존재하는 것을 확인할 수 있다. 국내의 경우 해외 항만 및 컨테이너 터미널과 비교하였을 때 직접적인 사이버 공격의 사례는 나타나지 않고 있다. 그러나 항만 및 컨테이너 터미널의 운영과 화물의 데이터 등을 전체적으로 관리하는 항만공사를 대상으로 발생되는 사이버 공격의 경우 증가하고 있다. 따라서 향후 국내 또한 항만 및 컨테이너 터미널을 대상으로 한 직접적인 사이버 공격 발생 가능성이 높다고 판단된다.

더하여 최근 항만 크레인을 통한 사이버 보안사고 가능성이 나타나고 있다. 미국 국방부 및 안보당국은 2023년 3월 중국 상하이진화중공업(ZPMC)가 생산한 초대형 항만 크레인을 통해 화물의 정보 유출이 될 수 있다고 발표했다. ZPMC는 중국에서 생산된 크레인 제조 업체로 선박에서 항만으로 컨테이너를 양·적하 시 화물의 출처 및 목적지를 추적할 수 있는 첨단 센서를 부착하고 있다. 2017년 ZPMC는 전 세계 모든 ZPMC 크레인 모니터링이 가능함을 언급하였으며 이를 바탕으로 미국 국방부는 크레인을 통해 미군 지원 화물에 대한 정보 유출 가능성을 제기하였다. 현재 ZPMC의 경우 전 세계 크레인 시장의 70%를 차지하고 있으며 미국의 경우 전체 STS 크레인의 80%를 판매한 것으로 파악되고 있다. 국내 또한 주요 항만 10곳에서 운용되는 크레인 중 절반 이상인 427기가 ZPMC 크레인을 사용하고 있다. 특히 국내 최대 항만인 부산항의 경우 538기 중 55.4%인 298기가 ZPMC 크레인이며 목포항, 포항항, 군산항, 마산항, 대산항 등 항만 5곳은 모두 ZPMC 크레인으로 운영되고 있다. 이러한 위험 제기에 따라 미국의 경우 ZPMC 크레인의 소프트웨어를 스위스 기업인 ABB 소프트웨어로 변경하였으며 국내 또한 국가정보원을 중심으로 중국산 크레인 전수조사 실시, 해양경찰 및 관련 기관의 적극적인 보안 점검을 진행하고 있다. 더하여 향후 개장 예정인 부산 신항 2-5단계, 2-6단계 컨테이너 전량을 국산 크레인으로 도입 계획을 밝혔다.

이렇듯 항만 및 컨테이너 터미널의 사이버 보안 공격 증가에 대응하기 위해 전 세계적으로 대응 전략 구축 및 사이버 보안의 규제·인증을 강화하고

있다. 미국의 경우 핵심 인프라 제어 시스템을 위한 사이버 보안 개선, 적극적인 파트너십 구축 등 전략적 동맹을 나타내고 있다. EU의 경우 러시아-우크라이나 전쟁으로 인하여 유럽 회원국의 사이버 보안 공격 급증에 따른 강력한 방어 능력 구축, 민군 협력 등 다양한 정책을 시행하였다. 해당 정책 시행으로 인하여 EU는 사이버 보안 규제 이행을 추진 및 모니터링 및 사이버보안위원회 설립을 추진하고 있다. 일본의 경우 2022년 정보통신, 항공, 철도, 공항, 물류, 화학 등 14개 국가 중요 인프라를 대상으로 사이버 공격이 각 인프라에 미치는 파급력을 도출하고 이를 고려하여 행동계획을 수립하였다. 국내의 경우 정보보호 산업 육성, 사이버 보안 기술 개발, 사이버 침해 사고 대응 체계 고도화 등 다양한 분야에서의 정책을 적극적으로 수립하고 있다. 특히 해양수산부, 국토교통부 등 관련 부처는 협력을 통하여 ICT 인프라 구축, 스마트 선박 · 항만(LTE-M)등 사이버 공격을 탐지 및 대응하는 차세대 보안 기술을 개발할 계획을 발표하였다. 이와 같이 점차 세부적인 기술적 대응 방안 개발을 통하여 향후 발생되는 사이버 공격에 신속한 대응이 가능할 것으로 기대된다.

사이버 위협에 대응하여 국가적 정책 뿐 아니라 항만 및 컨테이너 터미널 내에서도 적극적인 대응책을 모색하고 있다. 미국 LA 항만은 사이버 보안 위협 대응책을 수립하기 위하여 이해관계자를 중심으로 워킹그룹을 구성하였다. 이를 통하여 다양한 사이버 위협을 효율적으로 대비할 수 있으며 이해관계자 간 협력 및 정보공유를 통해 대응 능력 강화를 기대하고 있다. 네덜란드 암스테르담 항만은 항만 내 사이버 공격에 따른 디지털 복원력 향상을 위해 사이버 보안 프로그램을 운영하고 있다. 이를 통하여 사이버 위협 및 사고 정보의 즉각적인 공유가 가능하여 신속한 항만 사이버 보안 강화가 가능하다. 인천항의 경우 정보보호의 날을 제정하고 개인정보 침해 예방 및 정보보호 생활화를 위하여 IPA 직원을 대상으로 정보보안 교육 및 해킹메일 합동 모의훈련을 실시하고 있다. 부산항은 터미널 운영사와 공동으로 사이버 보안 협의회를 개최하였다. 또한 2019년부터 공동 사이버 공격 대응 훈련 등을 진행하고 있으며 향후 민간 협력 통해 사이버 보안을 강화할 예정임을 밝혔다.

Ⅲ. 선행연구 고찰

1. 항만 및 컨테이너 터미널 사이버 보안 관련 선행연구

Ignacio de la, P.Z.(2021)는 항만의 디지털 변화와 이로 인한 새롭게 위험 요소로 나타나고 있는 사이버 보안과 관련된 연구를 진행하였다. 사이버 보안과 관련된 문제의 경우 점차 스마트 항만의 확대에 따라 항만 산업에서 주요 관심사로 나타나고 있으나 항만 안전, 활성화 방안 등과 같은 타 분야에 비하여 여전히 연구가 미비한 상태다. 이에 사이버 위험을 보다. 객관적으로 평가하고 완화하는 방법론을 개발하고 사이버 공격에 따른 우선적 방어 및 복구 계획 구축 등과 같이 구체적인 방안이 필요한 상황이다. 본 연구는 사이버 보안과 관련된 연구의 필요성 언급 후 여러 방면에서의 시사점을 도출하였다. 우선적으로 경보 시스템 및 사이버 사고 대응 정책을 마련해야하며 위험 평가를 위한 새로운 조직 프레임워크 개발이 필수적이라고 언급하였다. 추가로 국제적으로 활발한 협력 강화 등 네트워크 구축이 필요하며 이러한 방안은 향후 항만과 터미널의 안전성을 확보 및 강화에 기여할 것이라고 설명했다.

B. Gunes, G. Kayisoglu and P. Bolat(2021)는 디지털화의 발전으로 서비스 및 인프라 사용에 있어 편리함과 효율성을 제공하지만 반대로 보안 및 안전의 문제 또한 발생한다고 언급하고 있다. 이에 항만, 공항 등 사이버 공격에 있어 중요 인프라 보존의 중요도 또한 향상되고 있다고 말했다. 이에 본 연구는

터키에서 운영되고 있는 컨테이너 항만을 대상으로 통합 사이버 보안 위험 관리 모델의 평가 프로세스를 구현한 사례 연구를 제시하고 있다. 연구 결과 항만의 자산이 사이버 보안에 의해 영향을 받는 것으로 나타냈으며 항만 시설 내 IT 인력들의 인식이 제고되었으며 책임의식이 확보되었다. 본 연구는 컨테이너 터미널 사이버 보안의 평가 네트워크를 구축했다는 점에서 의의가 있으며 향후 연구과제로 타 지역의 컨테이너 항만의 프로세스 적용 후 결과를 도출할 필요성이 있다고 분석하였다.

M. Bocayuva(2021)는 디지털의 활성화로 인하여 점차 금융, IT와 같은 중요한 서비스 및 인프라에 막대한 영향을 미치고 있으며 점차 더 효율적인 운영이 강조되고 있다고 언급했다. 특히 항만의 경우 디지털의 영향을 많이 받는 인프라 중 하나로 나타나고 있다. 그러나 이러한 디지털 시대의 도래는 과거 존재하지 않았던 사이버 보안 위협이라는 새로운 위협을 초래하였고 이러한 문제는 단순한 항만 내의 문제가 아닌 국민의 안전과 국가적 경제까지 영향을 미칠 수 있다. 특히 코로나-19로 인하여 과거에 비하여 디지털 의존성이 증가하고 있으며 선박 산업에서 사이버 공격이 약 4배가량 증가하였음을 밝혔다. 이러한 외부 환경에 따라 본 연구는 항만의 사이버 보안 투자가 적극적으로 나타나야 할 필요성이 존재하며 국가 기관과 민간기관 또는 국가 간 활발한 국제적 협력을 통하여 디지털 사이버 보안을 강화하는 것이 필요하다고 주장했다. 특히 본 연구는 유럽의 항만을 중심으로 연구를 진행하였는데 사이버 보안과 관련된 연구는 지속적으로 발전하였으나 여전히 항만과 관련된 규정은 모호한 상황이라고 밝혔다. 이에 현재는 보다 진취적으로 사이버 보안에 투자하고 해결책을 모색하여 취약성 감소가 시급한 실정이라고 언급하였다.

2. 타 산업 사이버 보안 관련 선행연구

송병호(2013)는 정보화가 빠르게 확산되는 시점에서 이를 악용한 범죄가 증가되고 있음을 주장했다. 또한 범죄의 수법이 점차 체계화되고 교묘해짐에 따라 국가 및 기업의 전반적 기반을 붕괴할 수 있는 위협 또한 증가하고 있다고 밝혔다. 이러한 피해의 경우 단순한 데이터 유출 뿐 아니라 기업 및 국가의 경제적, 인적 피해까지 확산 가능성이 존재한다. 그러나 현재 관련 법률의 경우 종합적이고 체계적이지 않다는 한계점이 존재한다. 따라서 보다 효과적인 법 집행이 이루어질 수 있도록 명확한 법적 근거를 정비해야할 필요성이 있음을 언급하였다. 더하여 공공부문과 민간부문에서 실질적으로 대응이 가능한 제도 모색, 위기관리 체계 구축을 통해 정교해지는 사이버 보안 범죄를 대응해야 할 필요성을 강조했다. 이에 본 연구는 사이버테러리즘의 변화에 대응한 보안기관과 수사기관의 대응강화 방안에 대하여 분석을 진행하였다. 이에 사이버 테러의 대응체계 강화, 국가협력 강화, 현행 법 · 제도 보완 필요, 민간 부문의 신고 의무화 등 다양한 분야에서의 시사점을 도출하였다.

오일석(2014)은 사이버 위험의 경우 개인이나 특정한 기관에서 대응하기 어렵기에 위험 조정 및 통합할 수 있는 기관을 중심으로 국가 차원의 대응 체계 구축 운영의 필요성을 주장하고 있다. 현재 주요 국가의 경우 사이버 보안을 국가적 정책에 추가하여 지속적인 정책 수립 및 기술 개발을 진행하고 있다. 하지만 여전히 국내의 경우 사이버 위험 및 보안 활동의 경우 비교적 소극적인 형태임을 밝혔다. 이에 본 논문은 국외 보안기관의 사이버 보안 및 정보통신기반 보호와 관련된 활동을 검토하고 국내 보안기관 활동과 비교 분석하였다.

이창규(2019)는 금융기관에 대한 사이버 보안 범죄의 경우 조직적인 범죄 집단의 출현으로 인하여 피해가 나타나고 있음을 언급하였다. 이에 본 논문은 국가 차원의 선제적 대응 방안이 필요하다고 판단하였다. 이에 사이버 금융 보안 정책의 경우 위협에 대한 높은 대응력 및 안정성을 보유한 영국의 금융 보

안 정책을 분석하여 향후 국내 금융기관의 사이버 보안 대처 방안을 살펴보고자 하였다. 현재 영국 정부의 경우 사이버 보안 인증 제도 실시, 기업 간 정보공유 프로그램을 통하여 보안 경쟁력을 향상시키고 있다. 또한 컴퓨터 긴급 대응 팀을 신설하여 국가적 차원의 금융 보안 역량을 높이고 국제 교류 확대 및 전문적인 인력 육성 등 다양한 교육 프로그램을 진행하고 있다. 이를 토대로 본 연구는 사이버 공격에 대응한 정부부처 및 민간부문 간 협력 강화, 사이버 공격에 대한 대응 방안 마련, 국제 협력 강화, 전문 인력 양성 등을 통해 금융 분야의 사이버 보안 범죄에 대응해야 한다고 분석하고 있다.

이지은(2020)은 4차 산업 기술과 함께 헬스케어와 포함되는 보건, 의료 등이 융합된 스마트 의료 분야의 혁신적 성장으로 인하여 의료기기 및 유전체 해킹 등 여러 방면에서 사이버 보안 문제가 발생하고 있음을 밝혔다. 특히 의료기기 해킹의 경우 단순한 고객의 개인정보뿐 아니라 질병과 같은 민감한 정보와 연관되어 있어 블랙마켓에서 고가로 매매될 가능성에 대해서 언급하였다. 이에 스마트 의료 보안과 관련된 국내외 가이드라인을 비교 분석 및 유사 융·복합 산업인 금융 산업의 보안과 비교 분석을 진행하였다. 분석 결과를 바탕으로 본 논문은 지속적인 정책 지원, 의료 ISAC에 대한 기능 범위 확대 및 지원정책 등 여러 방면에서의 정책적인 시사점을 도출하였다.

이은수·박성호(2021)는 4차 산업혁명 기술의 발전으로 아날로그 방식인 기존의 시스템에서 선박의 운영 시스템이 네트워크로 연결되어 디지털 방식으로의 변환 양상을 밝혔다. 더하여 지속적인 선박 운항시스템의 사이버 공격이 발생하여 국제해사기구 및 각국의 선급이 발표한 선박 사이버 보안 강화를 위한 지침 발표를 하였으나 국내의 관련 법제 및 대응은 여전히 미흡하다고 언급하고 있다. 따라서 본 연구는 선박 사이버 보안 강화를 위한 법제 정비 및 구체적인 사이버 보안 문제점에 대한 대응책 마련이 필요함을 목적으로 하고 있다. 이에 사이버 보안과 관련된 국제적인 대응책을 우선적으로 살펴본 후 국내 사이버 보안 법제 문제점을 도출한 후 개선점을 도출하였다.

김주미, 이민환, 이재훈(2022)은 최근 중소기업과 제조업을 대상으로 지속적인 해킹 피해가 있었으나 여전히 사이버 보안의 인식은 낮으며 특히 우리나라 중소제조업의 사이버 보안 대비는 미온적임을 밝혔다. 이에 본 연구는 국내외 사이버 보안 피해와 관련된 사례를 살펴보고 제조업 분야의 중소기업을 대상으로 실태조사를 실시하였다. 분석 결과 사이버 침해를 받은 기업의 96.7%가 악성코드에 감염되었음에도 불구하고 관련 규정 수립은 소극적인 태도를 보이고 있다. 또한 보안과 관련된 규정 수립의 필요성을 느낀 기업은 81.7%이나 실제 이와 관련된 규정이 수립된 기업은 41.8%로 매우 낮게 나타났다. 이에 본 연구는 사이버 보안에 대하여 중소기업의 사이버 보안에 대한 인식과 역량을 고려하여 정부의 정책 방향성을 도출하였다.

김현희·이대성(2022)은 원자력 시설의 사이버 보안 강화를 위한 훈련체계 개선방안에 관한 연구 정보처리기술의 발달을 통해 원자력 발전소의 사이버 위협 또한 증가하고 있음을 밝혔다. 이에 본 연구는 관련된 문헌조사 분석을 통하여 원자력 시설의 사이버 보안과 관련된 법령 및 체계의 개선방안을 도출하고자 하였다. 분석 결과 보안조치 관리의 단계적 접근방식이 필요하며 단기적으로는 훈련체계 개선, 사이버사고 대응 훈련 정책 규제 방안 제시 등의 세부적인 방안을 도출했다. 본 연구는 현재 진행되고 있는 원자력 시설의 사이버 보안 체계에 추가 개선 방안을 도출하였으며 이는 향후 궁극적으로 체계 개선에 기초 연구로 활용될 수 있다는 점에서 의의를 지닌다.

고기성·장영현·박인수·고진환(2023)은 전 세계적으로 4차 산업 기술의 도입에 따라 사이버 위협 역시 점차 고도화 및 정교화됨을 언급하였다. 이에

소프트웨어의 발전으로 항공기 시스템도 점차 디지털화됨에 따라 사이버 분야에서의 불안전한 영역으로 속해지게 되었음을 나타냈다. 이에 본 논문은 선진적으로 사이버 보안의 대응책을 마련한 미국 해군의 제도 및 사례 조사를 분석하여 국내 군용기에 적용될 수 있는 사이버 보안 제도 기틀을 구축하고자 하였다.

김진민 · 위성승 · 김낙일 · 신용태(2023)는 4차 산업혁명 및 신기술의 발전과 코로나-19에 따라 디지털 전환이 가속화되고 있음을 언급하였다. 더하여 이러한 변화에 따라 소프트웨어 공급망 해킹 피해가 점차 증가하고 있으며 향후 해킹 유형이 단순한 해킹이 아닌 대규모 해킹 형태로 변화할 가능성이 있음을 주장했다. 이에 본 논문은 우선적으로 주요 공급망 해킹 피해 사례를 조사하고 주요 보안 문제점을 파악하였다. 이후 주요국의 보안 관련 법제 및 표준 비교 및 분석하여 현재 국내 보안정책에 대한 시사점을 도출하였다. 분석 결과 국내 보안정책의 경우 법적 정비, 국가보안표준 및 평가체계 방안 등 정책적인 개선이 필요한 것으로 나타났다.

하도연(2023)은 최근 전 세계에서 발생되는 항만 및 컨테이너 내 사이버 보안 사고에 대하여 대응 방안을 도출할 필요가 있음을 언급하였다. 이에 부산항 컨테이너 터미널을 중심으로 강화 요인을 도출하였다. 분석 결과 부산항 컨테이너 터미널 사이버 보안을 위한 요인은 네트워크 구축 및 정책 지원, 교육 표준화 및 인력 양성, 법 · 제도적 요인로 구분되었다. 이후 다중회귀 분석을 통하여 안전성 확보 및 강화, 신뢰성 확보 및 강화, 성과 및 만족도 향상을 위한 세부 요인을 도출하였다.

3. 선행연구와의 차별성

앞서 선행연구 고찰을 통하여 항만 및 컨테이너 터미널 산업과 타 산업의 사이버 보안과 관련된 선행연구를 살펴보았다. 이를 통하여 해외에 비하여 국내에서 진행된 사이버 보안과 관련된 선행연구의 경우 타 산업을 대상으로 한 연구가 활발하게 나타난 것을 확인할 수 있었다. 이에 국내의 항만 및 컨테이너 터미널의 사이버 보안과 관련된 연구가 필요한 것을 판단하였다. 이에 본 연구에서는 부산항 컨테이너 터미널을 대상으로 사이버 보안 강화를 위한 우선순위를 도출하였다는 점에서 기존 연구와 차별성을 지닌다.

IV. 실증 분석

1. 분석 개요

본 연구를 수행하기 위하여 부산항 컨테이너 터미널 종사자 및 이해관계자를 대상으로 설문조사를 실시하였다. 설문 기간은 2023년 9월 7일부터 2023년 9월 27일까지 진행되었다. 설문 응답의 경우 총 98부를 회수하였다. 회수된 설문지 중 중복 응답 2부, 대답이 불성실한 응답지 6부를 제외하여 총 90부의 설문응답 데이터를 바탕으로 분석을 진행하였다. 설문 응답자의 일반 현황은 다음과 같다. 연령의 경우 60세 이상 0명(0.0%), 50~60세 7명(7.78%), 40~50세 25명(27.78%), 30~40세 34명(37.78%), 30세 이하 24명(26.67%)로 30세~40세가 가장 높게 나타났다. 현재 근무 업종의 경우 대학 및 연구원 18명(20.00%), 터미널 운영업체 33명(36.67%), 해운기업 및 선사 24명(26.67%), 항만공사 및 관련 공기업 15명(16.67%)로 나타났다. 근무연수의 경우 10년 이상 36명(40.00%), 5~10년 15명(16.67%), 3~5년 13명(14.44%), 1~3년 20명(22.22%), 1년 이하 6명(6.67%)로 나타났다. 근무 연수 중 10년 이상 근무한 응답자가 40%로 가장 높게 나타났으며 이를 통해 설문조사 결과의 신뢰성과 객관적인 대표성을 확보하였다. 설문조사에 사용된 부산항 컨테이너 터미널 강화 요인은 부산항 컨테이너 터미널 사이버 보안 강화를 위한 요인분석연구(하도연, 2023)에서 도출한 요인을 사용하였다.

표 1. 부산항 컨테이너 터미널 사이버 보안 강화요인

구분	요인	
네트워크 구축 및 정책 지원	A1	조직적 프레임워크 개발 및 조정
	A2	지속적인 사이버 보안 관련 정책 수립
	A3	이해관계자 간 협력
	A4	사이버 범죄 전담 대응 기구 확대
	A5	적극적인 투자 및 예산 증대
	A6	국·내외 상호 네트워크 구축
교육 표준화 및 인력 양성	B1	사이버 공급망 보안표준 제정
	B2	사이버 훈련 체계 구축
	B3	기존 인력 사이버 보안 교육
	B4	합동 대응 훈련 시행
	B5	사이버 보안 전문 인력 양성
법·제도적	C1	보안 관리체계 법적 정비
	C2	구체적인 규제 및 전략방안 수립
	C3	보안 인식 제고 및 보안 문화 확산
	C4	위협정보 공유체계 구축
	C5	사이버 위협 대응 체계 구축

자료 : 하도연(2023)

2. 분석 방법

아이젠하워 매트릭스 분석은 우선순위를 관리하고 결정하기 위한 분석방법이다. 각 요인의 산출 값은 X축의 시급성, Y축의 중요도에 배치되며 속성들의 평균치에 대한 산술평균을 원점으로 사용한다. 일반적으로 2x2 행렬 형태로 표현된다. 1사분면의 경우 즉각적으로 도입해야 할 영역이다. 2사분면의 경우 각 요인을 도입 및 수행하기 위한 계획과 전략을 수립해야 할 영역이다. 3사분면은 연기가 필요한 영역이며 4사분면의 경우 요인을 위임이 필요한 영역이다. 그러나 아이젠하워 매트릭스의 경우 2x2 매트릭스에 요인의 우선순위를 표현하기 때문에 세부적으로 각 요인의 우선순위를 도출할 수 없다는 한계점을 가진다. 따라서 본 연구에서는 세부적으로 각 요인의 우선순위를 살펴보기 위하여 Borich 요구도 분석을 추가적으로 실시하였다.

요구는 현재 수준과 바람직한 수준의 차이를 나타내는 것으로 두 수준의 차이를 체계적으로 분석하는 것이다. 요구분석은 매트릭스 분석에서 도출할 수 없는 요인의 우선순위를 세부적으로 도출할 수 있다. 이러한 요구분석의 경우 t 검정, Borich 요구도, The Locus for Focus Model 등이 있다. 본 연구는 Borich 요구도 분석을 진행하였다. Borich 요구도 분석의 경우 현재 수준과 요구 수준을 확인하고 가중치를 두어 결과 값을 산정하는 방법이며 기존의 T-test의 한계점으로 나타나는 두 항목 간 단순 차이 비교를 보완하고 요인 간 변별성을 제시한다. Borich는 중요하다고 인식하는 중요도 수준이 높고 성취도 수준이 낮을 때 요구도의 값이 높아지며, 요구도 값이 높게 나오는 것은 우선 증진이 필요함을 의미한다.

Ⅴ. 분석 결과

1. 아이젠하워 매트릭스 분석

부산항 컨테이너 터미널의 사이버 보안 강화를 위한 요인의 전반적인 우선순위를 시각화하기 위하여 우선적으로 아이젠하워 매트릭스 분석을 실시하였다. x축과 y축은 각각 요인의 시급성과 중요도로 설정하였으며 시급성(x축)의 평균값은 3.956으로 나타났으며 중요도(y축)의 평균값은 4.276으로 나타났다.

분석 결과 높은 시급성과 높은 중요도로 즉시 진행해야 할 필요성이 있는 1사분면에는 A3 (이해관계자 간 협력), C1 (보안 관리체계 법적 정비), C2 (구체적인 규제 및 전략방안 수립), C3 (보안 인식 제고 및 보안 문화 확산), C4 (위협정보 공유체계 구축), C5 (사이버 위협 대응 체계 구축) 요인이 구성되었다.

1사분면에 포함되는 요인을 살펴보면 대부분 법·

제도적 요인으로 나타나고 있다. 이를 통하여 현재 부산항 컨테이너 터미널 이해관계자들은 항만 사이버 보안 강화를 위하여 법·제도적 요인을 가장 중요하게 판단하고 있음을 확인할 수 있다. 즉시 처리 영역의 경우 조직에 직접적인 영향을 미치기 때문에 보다 즉각적인 대응이 필요하다. 따라서 보안 관리체계를 법적 강화 및 사이버 위협 대응 체계 구축에 중점을 두어야하며 보안 인식 제고 프로그램을 운영하거나 각 구성원들의 업무 특성을 고려한 맞춤형 교육을 통하여 산업 종사자에게 보안 인식 제고가 우선적으로 필요할 것으로 판단된다.

2사분면의 경우 A2 (지속적인 사이버 보안 관련 정책 수립) 요인이 구성되었다. 2사분면에 포함되는 요인을 살펴보면 네트워크 구축 및 정책 지원요인으로 나타나고 있다. 이를 통하여 현재 부산항 컨테이너 터미널 이해관계자들은 항만 사이버 보안 강화를 위하여 네트워크 구축 및 정책 지원 중 사이버 보안 관련 정책 수립은 중요한 요인이나 즉시 해결할 필요는 없다고 판단하고 있음을 확인할 수 있다. 기한 설정 영역의 경우 중요하고 가치 있는 일이나 시급하지는 않은 요인이기 때문에 보다 중장기적 관점에서 관리가 필요하다. 따라서 컨테이너 터미널 사이버 강화를 위한 중·장기적인 목표로 설정하여 변화하는 사이버 보안의 흐름을 충분히 파악하여 정책을 수립할 필요가 있다.

3사분면의 경우 A1 (조직적 프레임워크 개발 및 조정), A4 (사이버 범죄 전담 대응 기구 확대), A6 (국·내외 상호 네트워크 구축), B1 (사이버 공급망의 보안표준 제정), B2 (사이버 훈련체계 구축), B4 (합동 대응 훈련 시행) 요인이 포함되었다. 3사분면에 포함되는 요인을 살펴보면 네트워크 구축 및 정책 지원 요인과 교육 표준화 및 인력 양성 요인에 포함되는 요인으로 나타나고 있다. 특히 인력 양성의 요인 중 인력 양성과 관련된 요인을 제외하고 모두 3사분면에 속한 것을 확인할 수 있다. 이를 통하여 현재 부산항 컨테이너 터미널 이해관계자들은 항만 사이버 보안 강화를 위하여 네트워크 구축 및 정책 지원과 인력 양성 요인의 경우 축소 및 연기 필요성을 판단하고 있음을 확인할 수 있다. 삭제 영역의 현재 시점에서 관련성이 낮거나 중요도가 낮은 요인이기 때문에 간소화가 필요하다. 따라서 본 영역에 포함된 요인의 경우 부산항 컨테이너 터미널 사이버 강화를 위한 장기적인 목표로 설정할 필요가 있다.

마지막으로 높은 시급성과 낮은 중요도로 위임 필요성이 있는 4사분면에는 A5 (적극적인 투자 및 예산 증대), B3 (기존 인력 사이버 보안 교육), B5 (사이버 보안 전문 인력 양성) 요인이 구성되었다. 4사분면에 포함되는 요인을 살펴보면 대부분 교육 표준화 및 인력 양성 요인으로 나타나고 있다. 이를 통하여 현재 부산항 컨테이너 터미널 이해관계자들은 항만 사이버 보안 강화를 위하여 인력 양성 요인과 적극적인 투자 및 예산 증대의 경우 장기적인 목표에는 크게 영향을 주지 않는다고 판단하고 있음을 확인할 수 있다. 위임 영역의 경우 현재 시점에서는 중요도가 높지 않기 때문에 직접 처리보다 다른 전문 집단에 위임을 통하여 전략적인 운영이 필요하다. 따라서 특정 부서 혹은 전문가에게 해당 업무를 위임하거나 외부 업체와 협력을 통하여 효율적인 운영이 진행될 필요가 있다. 아래 그림은 아이젠하워 매트릭스 분석 결과이다.

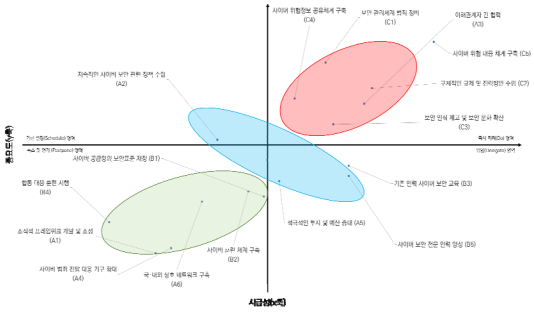

그림 1. 아이젠하워 매트릭스 분석 결과

자료 : 저자 작성

2. Borich 요구도 분석

아이젠하워 매트릭스 분석의 경우 전반적인 우선순위 도출은 가능하나 중심축에 근접한 항목에 대한 해석이 어렵다는 한계점을 가진다. 이에 Borich 요구도 분석을 진행하여 명확한 요인별 우선순위를 도출하였다. 분석 결과 C1 (보안 관리체계 법적 정비) 요인이 가장 높은 우선순위로 나타났으며 다음으로 A2 (지속적인 사이버 보안 관련 정책 수립), C4 (위협정보 공유체계 구축), B4(합동 대응 훈련 시행), C5(사이위협 대응 체계 구축) 등 순으로 나타났다. 반면 B5 (사이버 보안 전문 인력 양성) 요인이 가장 낮은 우선순위로 나타났으며 다음으로 B3 (기존 인력 사이버 보안 교육), B1(사이버 공급망 보안표준 제정), A5(적극적인 투자 및 예산 증대), A4(사이버 범죄 전담 대응 기구 확대) 등의 순으로 나타났다. 특히 우선순위가 높게 나타난 대부분의 요인은 법·제도적 요인에 속하는 것으로 나타났다.

표 2. Borich 요구도 분석 결과

우선순위		요인	시급성	중요도	중요도-시급성	Borich 요구도
1	C1	보안 관리체계 법적 정비	4.02	4.48	0.456	2.040
2	A2	지속적인 사이버 보안 관련 정책 수립	3.87	4.31	0.444	1.916
3	C4	사이버 위협정보 공유체계 구축	3.98	4.40	0.422	1.858
4	B4	합동 대응 훈련 시행	3.71	4.13	0.422	1.744
5	C5	사이버 위협 대응 체계 구축	4.18	4.52	0.344	1.558
6	C2	구체적인 규제 및 전략방안 수립	4.09	4.42	0.333	1.474
7	A6	국·내외 상호 네트워크 구축	3.84	4.18	0.333	1.393
8	A3	이해관계자 간 협력	4.08	4.39	0.311	1.365
9	C3	보안 인식 제고 및 보안 문화 확산	4.03	4.34	0.311	1.352
10	B2	사이버 훈련 체계 구축	3.91	4.20	0.289	1.213
11	A1	조직적 프레임워크 개발 및 조정	3.78	4.07	0.289	1.175
12	A4	사이버 범죄 전담 대응 기구 확대	3.80	4.08	0.278	1.133
13	A5	적극적인 투자 및 예산 증대	3.96	4.22	0.267	1.126
14	B1	사이버 공급망의 보안표준 제정	3.93	4.19	0.256	1.070
15	B3	기존 인력 사이버 보안 교육	4.06	4.26	0.200	0.851
16	B5	사이버 보안 전문 인력 양성	4.06	4.23	0.178	0.753

자료 : 저자 작성

이는 사이버 공격의 고도화됨에 따라 국가적 도적 요인에 속하는 것으로 나타났다. 차원의 체계적 대응 필요, 부처별 대응으로 인한 역할의 혼선, 업무 중복 등으로 인한 비효율화를 방지하기 위한 국가 차원의 운영이 필요하다고 판단된다. 반면 우선순위가 낮은 요인들은 대부분 교육 표준화 및 인력 양성 요인에 속하는 요인에 속하는 것으로 나타났다. 이는 정보보호 인력 관리체계의 미비, 전문가의 부족으로 교육 및 인력 양성의 제한, 실제 기업의 요구와 교육 간의 격차 등으로 인해 다른 요인에 비하여 다소 낮은 우선순위가 도출되었다고 판단된다.

VI. 결 론

1. 연구 요약 및 시사점

최근 항만은 항만 운영의 효율성 향상, 운영비 절감 등을 위하여 4차 산업 기술을 적극적으로 활용하고 있다. 이에 항만은 점차 자동화, 스마트 항만 등과 같이 더욱 발전된 모습으로 변화하고 있다. 그러나 이러한 항만의 변화에 항만 내 사이버 보안 공격이 증가하고 있다. 항만은 국가중요시설로 지정되어 있으며 사이버 공격으로 항만 내 업무 마비 및 테러 등이 발생 경우 단순한 업무 마비 및 운영 중단뿐 아니라 화물의 분실 및 손상과 같은 물리적 영향 사고로 이어질 수 있다. 또한 항만은 국가 전체의 수출입 관문 역할이며 특히 국내의 경우 항만의 역할이 더욱 크기 때문에 국가 전체의 경제적, 안전 위험으로 확대될 수 있다. 따라서 항만 사이버 보안 사고에 선진적으로 대응하기 위하여 구체적인 대응 방안 구축이 이루어져야 할 것으로 판단하였다. 이에 본 연구는 세계 7위의 컨테이너 항만인 부산항을 연구 대상으로 선정하였으며 항만 내에서 가장 자동화, 디지털화가 활발하게 나타나고 있는 컨테이너 터미널을 대상으로 분석을 실시하였다. 분석 결과를 요약하면 다음과 같다.

아이젠하워 매트릭스 분석 결과 1사분면의 경우 사이버 위협 대응 체계 구축, 구체적인 규제 및 전략 방안 수립 등이 속하였다. 이를 통하여 1사분면의 경우 법·제도적인 요인이 주로 포함되어 있음을 확인하였다. 2사분면의 경우 네트워크 구축 및 정책 지원 요인의 세부 요인인 지속적인 사이버 보안 관련 정책 수립이 속하였다. 3사분면의 경우 사이버 공급망의 보안표준 제정, 조직적 프레임워크 개발 및 조정 등이 속하였다. 이를 통하여 3사분면의 경우 교육 표준화 및 인력 양성 요인과 네트워크 구축 및 정책 지원 요인이 포함되어 있음을 확인하였다. 4사분면의 경우 기존 인력 사이버 보안 교육, 적극적인 투자 및 예산 증대 등이 속하였다. 이를 통하여 교육 표준화 및 인력 양성 요인 중 인력 양성 요인과 네트워크 구축 및 정책 지원 요인이 포함되어 있음을 확인하였다.

Borich 요구도 분석 결과 보안 관리체계 법적 정비가 가장 높은 우선순위로 나타났으며 다음으로 지속적인 사이버 보안 관련 정책 수립, 위협정보 공유체계 구축 등의 순으로 나타났다. 반면 가장 낮은 우선순위 요인은 사이버 보안 전문 인력 양성으로 나타났으며 다음으로는 기존 인력 사이버 보안 교육, 사이버 공급망의 보안 표준 제정 순으로 나타났다. 요인별로 살펴보면 법·제도적 요인이 대부분 높은 우선순위로 나타났으며 교육 표준화 및 인력 양성 요인이 대부분 낮은 우선순위로 나타났다.

분석 결과를 바탕으로 도출한 시사점은 다음과 같다. 첫째, 부산항 컨테이너 사이버 보안 강화 요인들에 대한 시급성과 중요도를 바탕으로 분석한 아이젠하워 매트릭스 결과를 살펴보면 즉시 시행 영역에서 모든 법·제도적 요인이 포함된 것을 확인할 수 있다. 이를 통하여 부산항 컨테이너 터미널 이해관계자들은 사이버 보안 강화를 위한 요인 중 법·제도적 요인이 가장 중요하게 인식하고 있음을 확인할 수 있다. 현재 국내에서는 「해사 안전법」과 「국제항해선박 및 항만시설의 보안 법률」을 시행하고 있다. 그러나 해당 법률의 경우 항만의 특성을 반영한 구체적인 내용 수립이 마련되지 않았다. 따라서 우선 현재 시행 중인 해사 안전법과 국제 항해선박 및 항만시설의 보안 법률을 바탕으로 최근 컨테이너 터미널에서 발생한 사이버 보안 위험 동향 및 추세 반영하여 법률 정비가 시급하다. 또한 항만 및 컨테이너 터미널의 사이버 보안의 강화는 보다 적극적인 이해관계자 간의 협력이 중요하다. 국가별 항만 사이버 보안 강화 및 대응 전략을 비교해보면 국내의 경우 국외에 비해 이해관계자 간 협력이 미비하며 사이버 위협에 대한 정보공유의 한계를 파악하였다. 특히 부산항의 경우 터미널 운영사와의 협의회 등 협력을

추진하고 있으나 향후 선사, 정책 입안자 등 더욱 다양한 이해관계자와의 협력을 추진할 필요가 있다. 항만은 방대한 데이터와 이해관계자들의 복잡한 관계가 나타나는 공간이다. 따라서 향후 부산항의 사이버 보안 강화를 위하여 이해관계자들의 적극적인 상호 협력이 필수적이다.

둘째, 아이젠하워 매트릭스 분석에서 위임 부분을 살펴보면 인력 교육과 관련된 요인이 포함된 것을 확인할 수 있다. 이를 통하여 부산항 컨테이너 터미널 이해관계자들은 전문가 및 관련 업체를 통하여 인력 교육 요인이 이루어지는 것이 효율적이라고 판단하고 있음을 확인할 수 있다. 현재 사이버 공격은 새로운 위협과 공격기술이 다양해지고 있어 인력 교육은 직원들의 보안 인식과 대응 능력을 향상하고 전문가 양성을 통하여 전문적인 분석과 위험관리가 필요하다. 그러나 인력 양성의 경우 전문성이 필요하며 자원과 교육 시간 등을 고려하였을 때 장기적인 시간을 요하기 때문에 전문 민간 기업, 사이버 보안 전문 교육 기관, 업체 등에 위임할 필요가 있다.

마지막으로, 부산항 컨테이너 사이버 보안 강화를 위한 요인에 대한 우선순위를 도출한 내용을 살펴보면 우선순위가 높은 요인은 대부분 법·제도적 요인으로 나타난 것을 확인할 수 있다. 반면 낮은 우선순위의 경우 대부분 교육 체계 및 인력 양성 요인으로 나타난 것을 확인할 수 있다. 이를 통하여 단계적으로 향후 사이버 보안 강화 및 대응 체계를 구축할 수 있다. 우선 법·제도적 요인의 경우 아이젠하워 매트릭스 분석에서 모두 즉시 시행 영역에 속하였으며 Borich 요구도 분석 모두 높은 우선순위로 도출되었다. 따라서 법·제도적 요인은 강화 및 대응 체계 구축에 있어 단기적인 목표로 설정할 필요성이 있다. 다음으로 네트워크 구축 및 정책 지원의 경우 아이젠하워 매트릭스 분석에서는 삭제 및 축소 영역에 속하였으며 Borich 요구도 분석에서도 몇 요인들이 다소 낮은 우선순위로 도출되었다. 따라서 네트워크 구축 및 정책 지원 요인의 경우 중·장기적인 목표로 설정해야 할 것이다. 마지막으로 교육 체계 및 인력 양성의 경우 아이젠하워 매트릭스 분석에서 위임 영역에 속하였으며 Borich 요구도 분석에서 대부분 낮은 우선순위로 도출되었다. 따라서 교육 체계 및 인력 양성 요인의 경우 향후 강화 및 대응 체계 구축에 있어 장기적인 목표로 설정해야 할 것이다.

2. 연구 한계점 및 향후 연구 방향

본 연구는 부산항 컨테이너 터미널이 사이버 보안에 대응하기 위한 요인의 우선순위 및 시사점을 다양한 방향으로 제시하였다는 의의를 지닌다.

그러나 본 연구는 부산항 컨테이너 터미널의 이해관계자를 대상으로 설문을 진행하였다. 하지만 이해관계자의 경우 실무자, 정책 입안자 등과 같이 구분될 수 있으며 각 집단은 업무의 특성이 다르기에 요인에 대한 인식 차이가 존재할 수 있다. 따라서 향후 연구에서는 이해관계자를 보다 세부적으로 구분하여 각 집단이 인식하는 컨테이너 터미널 사이버 보안 강화 요인에 대한 차이점을 분석할 필요가 있다.

참고문헌

강남선(2018), 선박 사이버 보안에 대한 기술적 분석, 한국마린엔지니어링학회지, 제42권 제6호, 463-471.

강다연·장명희(2012), 해운항만조직 구성원들의 정보보안 정책 준수에 영향을 미치는 요인, 한국항만경제학회지, 제28권 제1호, 1-23.

강다연·장명희(2014), 정보보안정책 준수가 정보보안능력 및 행동에 미치는 영향 분석 : 해운항만조직 구성원을 대상으로, 한국항만경제학회지, 제30권 제1호, 97-118.

강다연(2019), 항만물류조직구성원들의 보안능력에 영향을 미치는 요인, 한국항해항만학회지, 제43권 제3호, 179-185.

강동우·김기환·이영실(2022), 해양 사이버 보안사고 및 위험 관리 사항 동향, 융합신호처리학회 논문지, 제34권 제4호, 209-215.

강민구 · 김화영(2019), 항만보안 강화를 위한 평가요인과 상대적 중요도 분석, 한국항해항만학회지, 제43권 제1호, 49-56.

고현정(2011), 국제물류보안 인증제도 동향 및 시사점에 관한 연구, 한국항만경제학회지, 제27권 제2호, 333-354

김재광(2019), 항만 등 국가중요시설 민간경비체계의 법적 문제와 개선 방안, 공법학연구, 제 20권 제1호, 47-77.

김철준(2019), 해상보안 법체계의 개선방안에 관한 연구, 한국해양경찰학회보, 제9권 제1호, 24-44.

김태계(2013), 해상 · 항만에서의 테러행위규제에 대한 문제점과 대책, 법과정책연구, 제 13권 제2호, 499-534.

박상원 · 정민지 · 유윤재 · 윤경국(2022), IPA분석을 활용한 해상교통관제 인원의 사이버 보안 관리 인식 연구, 해양환경안전학회지, 제28권 제7호, 1140-1147.

배상균(2018), 일본 사이버 보안 정책에 관한 검토 – 사이버 시큐리티 기본법의 성립과 개정을 중심으로, 외법논집, 제42권 제2호, 141-165.

송병호(2013), 사이버 테러리즘의 변화에 따른 보안 · 수사기관의 대응강화 방안, 한국테러학회보, 제6권 제4호 75-92.

이경수 · 정현미(2019), 사이버 보안 관리도 패턴기반의 통합형 사이버 보안 위험관제 시스템, 학국컴퓨터정보학회논문지, 제24권 제11호, 99-107.

이대성(2019), 차세대 사이버 보안 동향, 한국정보통신학회논문지, 제23권 제11호, 1478-1481.

양천수 · 김중길(2019), 독일의 사이버 보안법 –정책 · 거버넌스 · 법률-, 법제연구, 제56권, 53-84.

이은수 · 박성호(2021), 선박 사이버보안 강화를 위한 입법론적 연구, 해사법연구, 제33권 제2호, 227-254.

이종찬, 이원영, 최준성, 왕핑, 국광호, 박상현(2016), 정부주도 사이버 보안 인력 양성 과정 개선 방안, 보안공학연구논문지, 제13권 제2호, 113-130.

이철원(2008), 국가 기반시설 사이버 보안기술 동향, Crisisonomy, 제4구너 제1호, 11-22.

전영은 · 김정연(2014), 금융회사의 사이버 보안 위협에 따른 개인정보보호 실태에 관한 연구, 한국IT서비스학회지, 제13권, 79-89.

전용태(2019), 중소기업의 기업경영 환경을 고려한 사이버 보안 관리, 시큐리티연구, 제59권, 9-36.

진쟁휘 · 왕치엔 · 김경래(2011), 중국항만시설 보안 문제점 및 개선방향에 관한 연구, 해양비즈니스, 제18권, 143-167.

하도연(2023), 부산항 컨테이너 터미널 사이버 보안 강화를 위한 탐색적 연구, 한국항해항만학회, 제 47권 제6호, 437-447.

Bunyamin G., Gizem K. and Pelin B.(2021), Cyber security risk assessment for seaports: A case study of a container port, *Computer and Security*, Volume 103.

Ignacio de la P.Z.(2021), Cyber security in ports and maritime industry : Reasons for raising awareness on this issue, *Transport Policy,* Volume 100, 1-4.

Manuela B(2021), Cybersecurity in the European Union Port Sector in light of the digital transformation and the COVID-19 Pandemic, *WMU Journal of Maritime Affairs,* 20(2), 173-192.

부산항 컨테이너 터미널 사이버 보안 강화를 위한 우선순위 분석

하도연 · 김치열 · 김율성

국문요약

최근 항만산업은 4차 산업혁명 기술을 적극적으로 도입하고 있으며 그 결과 자동화 항만, 스마트 항만 등 항만의 형태가 변화하고 있다. 이러한 변화는 항만의 효율성 증대와 같은 긍정적인 변화를 가져왔으나 그 반면 하역 장비를 통한 정보 유출, 랜섬웨어 공격에 의한 터미널 운영 중단 등 사이버 보안 사고 및 위협 가능성 또한 증가를 초래하였다. 항만의 사이버 보안 강화 방안의 우선순위를 제시할 필요가 있다고 판단하였다. 이에 본 연구는 국내 대표 항만인 부산항 중 가장 자동화가 빠르게 진행되는 컨테이너 항만을 대상으로 사이버 보안 강화 우선순위 도출 분석을 진행했다.

아이젠하워 매트릭스 분석을 진행한 결과 법 · 제도적인 요인이 1사분면에 주로 포함되어 있었으며 교육 체계 및 인력 양성 요인과 네트워크 구축 및 정책 지원 요인이 3사분면에 주로 포함되었다. 이후 Borich 요구도 분석을 실시한 결과 보안 관리체계 법정 정비가 가장 높은 우선순위를 나타냈으며 사이버 보안 전문 인력 양성이 가장 낮은 우선순위를 나타냈다.

본 연구는 향후 국내 컨테이너 터미널 사이버 보안 강화를 위한 기초연구자료로 사용될 것으로 판단된다. 또한 국내 컨테이너 터미널의 사이버 보안 강화 방안과 향후 국내 컨테이너 항만의 사이버 강화를 위한 선진적인 연구이며 향후 컨테이너 터미널이 나아갈 방향성을 제시했다는 점에서 의의를 지닌다.

주제어 : 부산항, 컨테이너 터미널, 사이버 보안, 우선순위