2019년 한국항해항만학회 추계학술대회
2019년 11월 20일(수)~21(목) 부산항국제전시컨벤션센터

해상분야 사이버보안 위험도 분석

유윤자* · † 박한선 · 박혜리** · 박상원***

*,**,***,† 한국해양수산개발원 해운해사연구본부

A Study on Cybersecurity Risk Assessment in Maritime Sector

Yun-Ja Yoo, † Han-Seon Park, Hye-Ri Park**, Sang-Won Park****

*,**,***,† Maritime Industry & Safety Research Division, Korea Maritime Institute, Busan 49111, Korea

요 약 : 국제해사기구(IMO)는 2017년 해상 사이버 위험관리 지침(Guidelines on maritime cyber risk management)을 발표했다. IMO의 해상 사이버 위험관리 지침에 따라 각 기국은 2021년 1월 1일 이후 도래하는 첫 번째 연차심사 전까지 안전관리규약(ISM, International Safety Management Code)의 선박안전관리시스템(SMS, Safety Management System)에서 사이버 리스크에 관한 사항을 통합·관리 하여야 한다. 본 논문에서는 해상분야의 사이버 보안 관리대상 및 위험요소를 식별하고 취약성 분석을 수행하기 위하여 IMO가 제시한 산업계 지침 및 국제표준을 근거로 해상분야의 사이버 보안 취약분야를 관리적·기술적·물리적 보안의 세 가지 영역으로 구분하였다. 또한, 리스크 매트릭스(Risk Matrix)를 사용하여 보안영역별 위험요소에 따른 정성적 리스크 평가(RA, Risk Assessment)를 수행하였다.

핵심용어 : 사이버 보안, 사이버 위협, 리스크 식별, 리스크 매트릭스, 리스크 평가

Abstract : *The International Maritime Organization (IMO) issued 2017 Guidelines on maritime cyber risk management. In accordance with IMO's maritime cyber risk management guidelines, each flag State is required to comply with the Safety Management System (SMS) of the International Safety Management Code (ISM) that the cyber risks should be integrated and managed before the first annual audit following January 1, 2021. In this paper, to identify cyber security management targets and risk factors in the maritime sector and to conduct vulnerability analysis, we catagorized the cyber security sector in management, technical and physical sector in maritime sector based on the industry guidelines and international standards proposed by IMO. In addition, the Risk Matrix was used to conduct a qualitative risk assessment according to risk factors by cyber security sector.*

Key words : *Cyber Security, Cyber Threat, Risk Identification, Risk Matrix, Risk Assessment*

1. 서 론

국제해사기구(IMO)는 해상 분야의 사이버 보안체계 강화 필요성을 논의해 왔으며, 결과로써 2017년 해상 사이버 위험관리 지침(Guidelines on maritime cyber risk management)를 발표했다. 동 지침에서는 선주단체 등의 산업계 지침과 ISO 국제표준 및 미국 국가표준기술원(NIST, National Institute of Standards and Technology) 기준을 추가적으로 제시했다 (BIMCO, 2018; IMO, 2017). .... (중략)····.

본 연구에서는 해상 분야의 사이버 보안 취약 분야를 관리적·기술적·물리적 보안 세 가지 영역으로 구분하고 ...

. (중략)····..

...

2. 사이버 보안 위험요소 식별

해상분야에서의 사이버 보안 위험요소 식별을 위해 산업계 지침 및 ISO 국제표준을 근거로 해상분야 사이버 보안 관리대상 및 위험요소를 식별한다.

····(중략)····.

2.1 관리적 보안대상 통제항목

산업계 지침 및 정보기술 국제표준인 ISO/IEC 27001에 근거한 관리적 보안대상의 사이버 위험에 대한 통제항목은 다음과 같다(ISO/IEC 27001, 2013)···· (중략) ·····..

... (중략).... .

† 종신회원, hspark@kmou.ac.kr
* 종신회원, yjyoo@kmi.re.kr

2.2 기술적 보안대상 통제항목

산업계 지침 및 정보기술 국제표준인 ISO/IEC 27001에 근거한 기술적 보안대상의 사이버 위험에 대한 통제항목은 다음과 같다(ISO/IEC 27001, 2013)···· (중략) ·····.

Table 1 Control objectives by cyber security area

Classification		Description
A1	Policy	...(중략)...
A2	Asset management	...(중략)...
...	...(중략)...	...(중략)...
T1	Network management	...(중략)...
...	...(중략)...	...(중략)...

····· (중략) ·····.

2.3 물리적 보안대상 통제항목

산업계 지침 및 정보기술 국제표준인 ISO/IEC 27001에 근거한 물리적 보안대상의 사이버 위험에 대한 통제항목은 다음과 같다(ISO/IEC 27001, 2013)···· (중략) ·····.

3. 해상분야 사이버보안 위험도 분석

해상분야에서의 보안 영역별 취약도 분석을 위해 .... (중략).... 항목에 대한 위험도를 조사하고 정성적 리스크(RA, Risk Assessment)를 평가하였다. ..

····(중략)····.

$$RA\ (Risk\ Assessment) = Likelihood \times Severity \quad (1)$$

3.1 관리적 보안 위험도

관리적 보안 위험도 결과 및 리스크 매트릭스 분석 결과는 다음과 같다.

····· (중략) ·····.

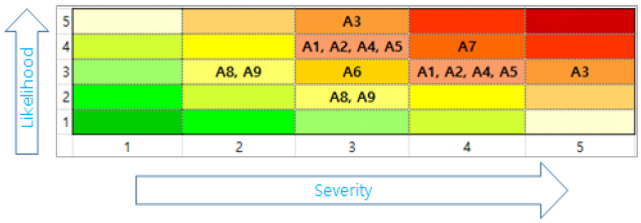

Fig. 1 Risk matrix of administrative security sector

3.2 기술적 보안 위험도

기술적 보안 위험도 결과 및 리스크 매트릭스 분석 결과는 다음과 같다.

····· (중략) ·····.

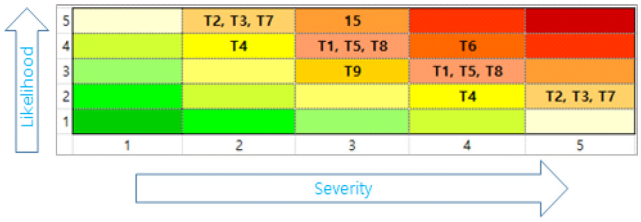

Fig. 2 Risk matrix of technical security sector

3.3 물리적 보안 위험도

물리적 보안 위험도 결과 및 리스크 매트릭스 분석 결과는 다음과 같다.

····· (중략) ·····.

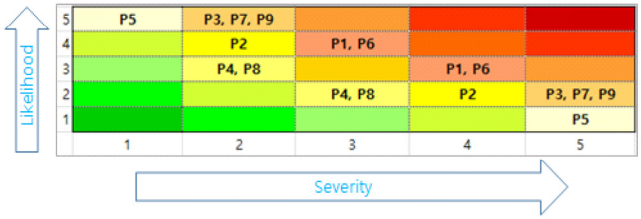

Fig. 3 Risk matrix of physical security sector

····· (중략) ·····.

4. 결 론

본 논문에서는 해상분야의 사이버보안 취약요소를 식별하고 보안 관리대상을 관리적·기술적·물리적 보안 영역으로 구분하

였다. 보안 영역별 취약성 분석을 위해 산업계 및 국제표준에서 제시한 보안 관리대상 통제항목을 근거로 정성적 위험도 평가를 수행하였다.

...(중략),,,

향후 ····· (중략) ·····.

참 고 문 헌

[1] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, WORLD SHIPPING COUNCIL(2018), The Guidelines on Cyber Security Onboard Ships, Version 3.

[2] IMO(2017), Guidelines on Maritime Cyber Risk Management, IMO MSC-FAL.1/Circ.3.

[3] ISO/IEC(2013), ISO/IEC 27001 standard on information technology, Annex A.