해사 사이버보안 동향 분석 및 해사 사이버보안 시스템 구축

안종우* · 임정규** · † 박개명

*,**한국선급, † 한국선급 사이버인증팀장

Maritime Cyber Security Status and Establishment of Maritime Cyber Security System

Jong-Woo Ahn · Jeoung-Kyu Lim** · † Kae-Myoung Park*

*,**Korean Register, Busan 46762, Rep. of Korea*
† Cyber Certification Team, Korean Register, Busan 46762, Rep. of Korea

요 약 : 정보통신기술의 발전으로 인하여 선박 내 시스템 간 또는 선박과 육상 시설 간의 정보 교환 및 통신이 용이하게 되어 업무 효율이 향상되고 있다. 그러나 이러한 회사와 선박의 업무 환경의 변화는 회사 및 선박의 시스템으로의 비인가된 접근 또는 악성코드 감염과 같은 사이버보안 사고 발생 가능성을 높이는 요인이 되어 안전, 환경 및 상업적으로 중대한 피해를 야기할 수 있다. 따라서 증가하는 사이버위협을 식별하고 대응하기 위하여 사이버 리스크 기반 접근법이 필요하게 되었다. 본 논문에서는 해사 사이버보안 동향을 분석하고 해상 사이버보안 시스템 구축을 위한 가이드라인을 제공하고자 한다.

핵심용어 : 해사 사이버 보안, 사이버보안 리스크 평가, 해사 사이버보안 시스템

Abstract : *The development of Information and Communication Technology facilitates exchange of information and communication between system in ships or between ships and land facilities, thereby improving the efficiency of their work. However, these changes in the working environment of companies and ships increased the likelihood of cyber security incidents occurance like unauthorized access to company and ship systems or infection of malicious code, which results in significant safety, environmental and business damage to company and ships. Therefore, a cyber-risk-based approach was required to identify and respond to an increasing cyber threats. In this paper, the analysis of maritime cyber security status and guidelines for establishment of maritime cyber security system are provided.*

Key words : *Maritime Cyber Security, Cyber Security Risk Assessment, Maritime Cyber Security System*

1. 서 론

정보통신기술의 발전으로 인하여 선박에 컴퓨터 기반 시스템이 광범위하게 사용되면서 선박의 시스템이 자동화, 통합화, 디지털화되고 있다. 이것은 선박 내 시스템 간 또는 선박과 육상과의 정보 교환 및 통신을 용이하게 만든 반면 사이버공격 빈도를 증가시켰다. 이에 따라 해사 분야에서의 사이버보안에 대한 중요성이 인식되면서 국제적으로 사이버 리스크 관리에 대한 관심이 높아지고 있다. 이 논문에서는 사이버 리스크 관리에 대한 국제적인 동향을 분석하고, 사이버 리스크를 관리하기 위한 방법에 대해서 살펴보고자 한다.

2. 국제 사이버보안 대응 동향

사이버 리스크 관리에 대한 국제적인 동향은 사이버보안 인식을 제고하고 체계적인 사이버보안 관리 시스템을 구축하기 위한 가이드라인 및 검사 요건을 개발하고 이를 구현하도록 요구하고 있다. 사이버 리스크 관리를 위한 국제 가이드라인 및 표준은 다음과 같다.

(1) The Guidelines on Cyber Security Onboard Ships
(2) ISO 27001 : Standards on Information Technology
(3) NIST Cyber Security Framework

2.1 국제해사기구(IMO)

IMO의 전반적인 목표는 사이버 리스크에 대해 운영상 탄력성을 유지하여 안전한 운송을 지원하는 것이다. 이를 위하여 2017년 MSC 98차 회의에서 해사 사이버 리스크 관리에 대한 가이드라인(MSC-FAL.1/Circ.3)을 발표하였고, 동 회의에서 2021년 1월 전에 선주와 선박 관리자에게 사이버 리스크를 선박 안전

† 교신저자 : kaemyoung@krs.co.kr
* ahnjwoo@krs.co.kr

관리시스템(SMS)에서 관리하도록 촉구하는 결의서(Resolution MSC.428(98))을 채택하였다. 이에 따라 많은 기국들이 2021년 이후 도래하는 검사에서 이를 확인할 것으로 예상된다.

2.2 국제선급협회(IACS)

IACS는 사이버보안에 대한 이슈를 체계적으로 논의하기 위하여 사이버시스템 패널을 2016년 신설하였으며, 선박 사이버시스템의 안전성을 보장하기 위한 12가지 핵심 기술에 대한 권고서를 2018년 발간하였다. 또한 한국선급을 비롯한 ABS, DNV-GL, LR 등 선급들은 사이버보안 가이드라인을 개발하여 배포하였으며, 선박에 사이버보안 부기부호(Notation)을 부여하는 서비스를 제공하고 있다.

2.3 국제해운업계

2016년 발틱국제해사위원회(BIMCO)를 주축으로 한 해운업계에서는 선박 사이버보안에 대한 가이드라인을 발간하였으며, 매년 개정안을 발표하고 있다. 이 가이드라인은 IMO에 보고되어 사이버 리스크 관리를 위한 기초 자료로 사용되고 있다.

국제 정유사 해운포럼(OCIMF)에서는 2018년부터 탱커선사 화주검사(TMSA 3)와 SIRE VIQ 7에 사이버보안 요건을 포함시켰으며, 광탄선운반선 화주검사(RIGTSHIP Inspection) 역시 사이버보안을 요구하고 있다.

3. 해사 사이버보안 시스템 구축

해사 사이버보안 시스템은 회사 및 선박의 사이버자산의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availablity)을 보증하기 위하여 리스크 기반 접근방법을 활용하여 사이버보안 리스크 및 사이버보안 취약성을 주기적으로 모니터링할 수 있도록 보안 대책을 마련하고 지속적인 개선이 가능하도록 절차를 개발하고 운영하는 종합적인 시스템을 말한다. 사이버보안 시스템은 크게 관리적 보안, 물리적 보안 및 기술적 보안으로 구분할 수 있다.

3.1 사이버보안 리스크 평가

사이버보안 리스크 평가의 목적은 식별된 자산에 대하여 사이버보안 수준을 지속적으로 향상시키기 위한 기반을 마련하는 것이다. 따라서 선박 및 회사의 중요 사이버 시스템에 대하여 사이버위협에 취약한 부분을 식별하고, 이에 대한 리스크 감소 방안을 마련하여 사이버보안을 강화하기 위하여 체계적인 리스크 평가 방법론을 사용하여야 한다. 이를 통하여 회사들은 현재 자신의 사이버보안 리스크 수준을 확인하고, 목표로 하는 리스크 수준과의 차이를 분석하여 사이버보안 수준을 향상시킬 수 있는 전략적인 결정을 내려야 한다.

사이버보안 리스크 평가의 첫 번째 단계에서는 리스크 평가 대상에 대한 명확한 이해를 위하여 필요한 정보를 수집하고, 리스크 평가의 목적, 범위 및 리스크 허용 수준 등 리스크 평가를 위한 필요 사항을 정의한다. 이 작업을 수행하기 위한 최소한의 정보는 다음과 같다.

(1) 네크워크 구성 및 구역 분류
(2) 대상 시스템 정보 : 하드웨어/소프트웨어 목록, 시스템 간 인터 페이스
(3) 리스크 허용 기준

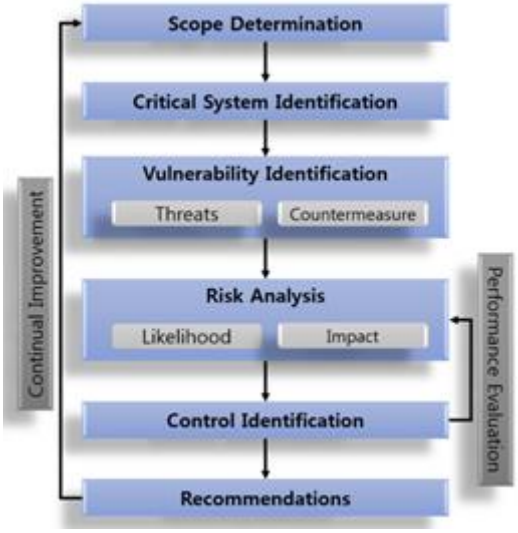

Fig. 1 Procedure for Cyber Security Risk Assessment

두 번째 단계는 회사나 선박의 시스템에 대해 기밀성, 무결성, 가용성을 기반으로 중요도(Criticality)를 결정하는 것이다. 중요도 인덱스(CrI)는 기밀성 인덱스(CoI), 무결성 인덱스(II), 가용성 인덱스(AI)의 합인 자산 중요도에 의해 아래 테이블과 같이 결정된다. 단, 이 논문에서는 인덱스의 값을 5로 하였으나, 다른 값으로 사용 가능하다.

Table 1 중요도 인덱스(CrI)

자산 중요도	카테고리	CrI
13 ≤ 자산 중요도 ≤ 15	Definite	5
10 ≤ 자산 중요도 ≤12	Probable	4
7 ≤ 자산 중요도 ≤ 9	Occasional	3
5 ≤ 자산 중요도 ≤ 6	Remote	2
3 ≤ 자산 중요도 ≤ 4	Improbable	1

세 번째 단계인 취약성 식별에서는 사이버 위협과 그로 인한 영향 및 사이버 리스크 완화 방법을 식별하여 다양한 사이버

위협 시나리오들을 식별할 수 있다. 취약성 식별은 시스템 정의 단계에서 식별된 각 시스템별 사이버위협 요소, 그로 인한 영향, 이미 적용된 리스크 감소 방법 및 추가 적용 가능한 방법을 식별하여 발생 가능한 모든 사이버 위협 시나리오 목록을 작성한다.

네 번째 단계인 리스크 분석은 식별된 사이버 위협 시나리오들의 리스크를 정성적 또는 정량적으로 표현하기 위해서 수행되며, 대상 시스템의 사이버보안 리스크를 확인하고 시스템 내부 사이버 위협에 취약한 부분을 검토할 수 있다. 정성적 리스크 분석 방법으로 빈도 지수(Frequency/Likelihood Index : LI)와 영향도 지수(Impact Index)를 리스크 인덱스(Risk Index : RI)로 표현하는 리스크 매트릭스(Risk Matrix)를 사용할 수 있다. 또한 충분한 데이터가 준비되어 있을 경우, 널리 통용되는 증명된 리스크 분석기법을 사용하여 정량적 분석을 수행할 수 있으며 이외에도 회사가 보유한 고유의 리스크 분석 방법을 적용하여도 무방하다. 이 논문에서는 빈도 지수는 위협 인덱스(Threat Index)와 취약성 인덱스(Vulnerability Index)를 기반으로 결정되었으며, 리스크 인덱스는 빈도지수와 영향도 인덱스인 중요도 인덱스의 곱에 의해 결정되었다.

Impact	5	5 Significant	10 Significant	15 Major	20 Major	25 Major
	4	4 Low	8 Significant	12 Significant	16 Major	20 Major
	3	3 Low	6 Significant	9 Significant	12 Significant	15 Major
	2	2 Low	4 Low	6 Significant	8 Significant	10 Significant
	1	1 Low	2 Low	3 Low	4 Low	5 Significant
Index		1	2	3	4	5
		Frequency				

Fig. 2 Risk Matrix

다섯 번째 단계는 리스크 저감시킬 수 있는 방법을 식별하는 것이다. 리스크 저감 방법은 사이버 위협의 발생 빈도를 줄일 수 있는 방법과 사이버 위협으로 인한 영향을 최소화할 수 있는 방법으로 구분될 수 있다. 단, 이 단계에서는 리스크 저감 방법에 대한 시급성, 가성비와 같은 필요성을 검토하여야 한다.

사이버보안 리스크 평가 보고서는 현재 사이버보안 리스크 수준과 리스크 저감이 필요한 영역, 리스크 저감을 위하여 요구되는 추가 방법들 및 리스크 저감 방법 적용 담당자를 쉽게 식별할 수 있도록 적절하게 작성되어야 한다.

3.2 관리적 보안

관리적 보안은 사이버보안 관리 조직 체계 수립, 사이버보안 지침과 절차 수립, 비상대책 수립과 사이버보안 사고 대응책 마련, 자산의 보안등급 분류 및 가치 평가 실시, 인사 상의 보안 관리 및 보안 교육 실시 등과 같이 조직을 운용하는데 필요한 관리 상의 보안 문제를 해결하는 것이다.

사이버 위협으로부터 대응하고 사이버보안 수준을 유지 및 향상시키기 위하여 회사는 우선적으로 사이버보안 조직을 구성하여야 한다. 선사의 사이버보안 조직 구성의 예는 다음과 같다.

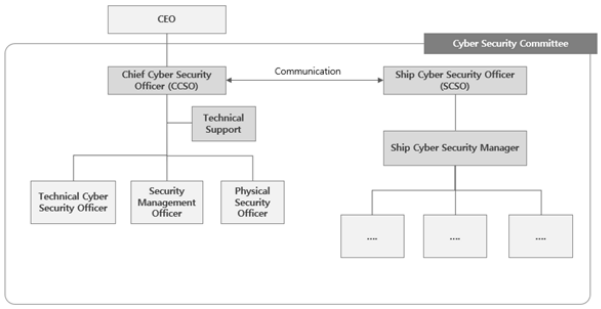

Fig. 3 Example of Cyber Security Organization in Shipping Company

3.3 기술적 보안

기술적 보안은 시스템을 구성하는 하드웨어와 소프트웨어의 기술적 요소들을 보안 상의 위협으로부터 안전하게 보호하기 위하여 새로운 시스템 환경에 맞도록 시스템 보안, 네트워크 보안, PC 보안 등 취약점을 진단하고 대책을 수립하는 것이다. 시스템 보안은 서버 보안, 시스템 접근 통제 등으로 구성되며 시스템을 기술적으로 보호해는 대책이다. 네트워크 보안은 방화벽, 가상사설망(VPN), 침입방지시스템(IPS), 침입탐지시스템(IDS) 설치 등을 통하여 네트워크로 접근 가능한 자산에 대한 보호대책이다. 만약 내부 네트워크가 아닌 외부 네트워크를 통해 선박 네트워크로의 접근이 불가피한 경우, 인가된 접속자를 식별하고 안전한 암호화된 통신이 이루어지도록 보안성을 강화하여야 한다.

3.4 물리적 보안

회사나 선박의 주요 시설에 설정된 보안 구역에 대한 위협과 자연재해로부터 보호하기 위하여 물리 및 환경 보안 기준을 적용하여 물리적 접근통제에 대한 분석 및 보호대책을 수립하여야 한다. 물리적 보안은 보호구역 통제, 물품의 반출입 통제, 설비 및 시설 관리, 환경 보안 등으로 구성된다. 물리적 보안은 업무의 중요도와 자산의 위치에 따라 보호 구역을 구분하고 구역별 보호 대책을 수립하여야 한다. 일반적으로 보호구역의 중요도와 특성에 따라 화재, 전력 이상, 비인가된 외부 침입 등을 방지하기 위하여 보호구역별로 온습도 조절기, 화재 감지 및 소화설비, 누수감지기, UPS 및/또는 비상발전기, CCTV 등을 갖추고 운영 절차를 마련하여야 한다.

4. 결　　론

컴퓨터 기반 시스템의 선박 적용 확대로 인한 스마트선박의 출현으로 자율운항선박 및 무인화선박 개발 등이 이루어지면서 해사업계에 사이버 시스템의 도입이 가속화되고 있다. 이로 인해 사이버 공격에 회사 및 선박이 노출되면서 사이버보안이 필수적으로 요구되고 있다. 따라서 사이버공격으로부터 회사와 선박의 사이버 자산을 안전하게 보호할 수 있는 사이버보안 시스템 구축 및 지속적인 개선 노력이 필요하다.

참 고 문 헌

[1] IMO(2017), “Guidelines on Maritime Cyber Risk Management”

[2] IMO(2017), “Maritime Cyber Rsk Mnagement in Safety Management Systems”

[2] BIMCO(2018), “The Guideline on Cyber Security onboard Ships”, Rev., 3

[4] Korean Register(2019), “Guidance for Maritime Cyber Security System“