Journal of the Korean Society of Marine Engineering, Vol. 42, No. 6 pp. 463~471, 2018
J. Korean Soc. of Marine Engineering (JKOSME)
https://doi.org/10.5916/jkosme.2018.42.6.463

ISSN 2234-7925 (Print)
ISSN 2234-8352 (Online)
Original Paper

선박 사이버 보안에 대한 기술적 분석

강남선†

(Received December 13, 2017 ; Revised January 5, 2018 ; Accepted May 29, 2018)

Analysis of onboard ship cybersecurity

Nam-Seon Kang†

요약: 본 논문에서는 선박의 사이버 보안 현황을 분석하고 국제해사기구, 국제표준화기구 등의 해상 사이버 보안에 대한 국제 동향을 파악하였으며, 선박 사이버 보안 가이드라인, 영국 선급의 해운산업에 대한 사이버 보안 가이드라인, 미국 선급의 선박 및 플랫폼에 대한 사이버 보안 가이드라인을 분석하였다. 가이드라인에서 제시된 사이버 보안에 대한 인식 개선, 이행 절차 수립, 기술, 교육 중 사이버 보안 기술을 다루며, 발표된 가이드라인 중 기술적 요구사항을 구체적으로 제시한 사이버 보안 가이드라인을 기준으로 선박 사이버 보안에 대한 기술적 구현방안을 보안이 강화된 네트워크의 구성, 선내 네트워크 통합 관리, 데이터 보안, 선박용 안티바이러스 서비스로 제안하였다.

주제어: 선박 사이버 보안, 선내 네트워크 통합 관리, 데이터 보안, 선박용 안티바이러스, 선박 사이버보안 가이드라인

Abstract: In this paper, we analyze the status of ship cyber security and identify international trends in the cybersecurity of international maritime organizations and international standardization organizations. We analyze the guidelines on cyber security aboard ships, cyber-enabled ships (Lloyd's Register), and cyber security principles of marine and offshore operations (American Bureau of Shipping). This article discusses cyber security technologies in areas of awareness improvement, implementation procedure establishment, technologies, and guidelines education. Regarding the specific technical requirements, this article suggests a security enhanced network, integrated onboard network management, data security, and anti-virus software as technical methods of realizing onboard-ship cyber security.

Keywords: Onboard-ship cyber security, Integrated onboard network management, Data security, Antivirus service for ship, Guideline on cyber security onboard ships

1. 서 론

스마트 선박의 출현, 디지털 통신 도입, 조선해양 IT기자재의 증가로 인해 선내 장비가 독립된 형태로 운영되던 과거와 달리 네트워크화 되고 있으며, 장비 간, 시스템 간 데이터를 공유하는 사례가 증가하고 있다**[1][2]**. 또한 국제해사기구(IMO, international maritime organization)의 e-Navigation 협약 이행이 가시화 되면서 선내 및 선육간 통신환경의 개선과 선박과 선박 간(ship to ship), 선박과 육상 간(ship to shore) 연계 기술 개발이 활발히 진행되는 등 해상 사이버 환경이 급격히 변화되고 있다**[3][4]**.

하지만 이러한 변화에도 불구하고 해운산업에서는 운송선박 및 항만 시설에 대한 해상 테러 대비 국제선박 및 항만시설 보안코드(ISPS, the international ship and port facility security code) 외의 선박 보안에 대비하지 않고 있어 IT 기술 확대에 따른 해상 사이버 사고 위험에 대한 경고가 이어지고 있다**[3][5]**.

영국 해운로펌인 홀맨 펜윅 & 밀란은 해운산업을 가장 확실한 사이버 테러의 표적으로 경고하였으며, USCG (united states coast guard)의 해상사이버 보안연구 결과 자동화 네트워크 설비가 많은 디지털 선박과 항만 터미널의 사이버 보안 위험도가 매우 높은 것으로 확인되었다**[5][6]**.

실제로 노르웨이 해양플랫폼에서 2015년 30건 이상의 사이버 사고가 감지되었으며, 석유 시추 중이던 오일 플랫폼의 위치가 해킹에 의해 아프리카 대륙으로 변조되어 시스템이 일시적으로 다운되는 사고가 발생하였다**[7]**. 소말리아 해적들은 선사의 사이버 시스템을 해킹해 선박의 화물과 보안상태를 확인하여 아덴만 운항 선박에 해적행위를 하고 있으며, 2017년 6월 27일 전 세계를 덮친 랜섬웨어 Petya 공격으로 세계 최대 해운선사인 A. P. Moller-Maersk 76개 터미널 중 63개가 마비되어 3억 달러의 손실이 발생되는 등 사이버

† Corresponding Author (ORCID: http://orcid.org/0000-0001-9740-2898): R&D team, Marineworks Co., Ltd. Saemunan-ro 5-gil 19, Jongno-gu, Seoul 03173, Korea, E-mail: ddalgi99ns@gmail.com, Tel: 02-6952-7251

공격에 의한 해상 보안 사고가 현실화 되고 있다**[7][8]**.

이처럼 높아지고 있는 해운산업에 대한 사이버 보안 사고에 대한 위험성을 알리고, 위험에 대응을 위해 해운단체, 산업체, 선급 등에서는 해운산업의 사이버 보안 문제를 다루기 위한 가이드라인 정립과 국제 규제 채택에 노력을 기울이고 있다. 또한 전 세계 주요 화주협회는 2018년부터 광탄운반선 화주검사(RIGHTSHIP), 탱커선 화주검사(TMSA) 시 선박의 '사이버 보안 대응절차' 보유 여부와 관리 사항을 점검항목에 포함시킬 것으로 발표하여 사이버 보안에 관한 해운선사의 대응방안 마련이 필요하다**[9]**.

본 논문에서는 선박 사이버 보안 가이드라인을 기준으로 선박 사이버보안과 해상 ICT 환경 개선을 위한 기술적 검토를 수행하고자 하며, 구성은 다음과 같다. 2장에서는 선박 사이버 보안 현황을 분석하고 3장에서 선급 및 관련 단체에서 개발되고 있는 선박 사이버 보안 규정에 대하여 분석한다. 4장에서 선박 사이버 보안 대응 기술의 요구조건을 도출하며 5장에서 결론을 제시한다.

2. 선박 사이버 보안 현황

2.1 선박 현황

현재 선박은 **Figure 1**과 같이 네트워크 상태 모니터링 시스템과 네트워크 보안 장비 부재, 소프트웨어 업데이트 부족 등으로 인해 다양한 사이버 위험에 노출되어 있다**[10]**.

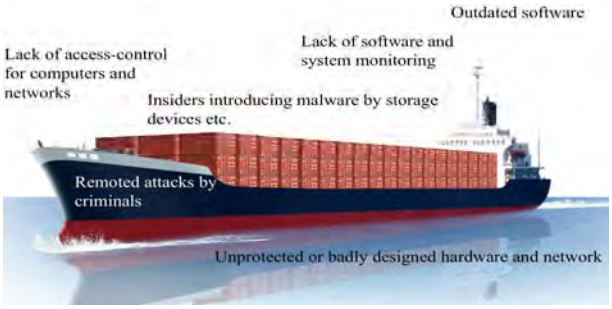

Figure 1: Risks on board ships **[10]**

첫째, 개방형 네트워크에 대한 보안 프로세스와 시스템이 부재하다. 지금까지 선박은 사이버 환경에서 야기되는 보안 사고를 방지하기 위해서 일부 선내 거주 공간과 업무용 PC에서만 선육 간 통신을 허용하도록 네트워크를 물리적으로 구분하여 운영하고 있다. 하지만 조선해양기자재가 IT화, 네트워크화 되면서 장비 간, 시스템 간 데이터 수집과 공유 등이 요구되고 있으며, 특히 e-Navigation 서비스 이행을 위한 선육 간 통신 등이 요구되고 있어 개방된 네트워크 환경에서 증가하고 있는 선박 IT 장비에 대한 관리 및 보안이 어려운 상황이다**[10]**.

둘째, 선박에 설치된 장비와 네트워크에 대한 상태 모니터링과 네트워크 장비 관리를 위한 시스템이 부재하다. 현재 선내 네트워크는 단순히 방화벽과 게이트웨이로 분류하고 있으며 네트워크 장비에 대한 모니터링 및 통합관리와 비인가 장치에 대한 관리 등이 이루어지지 않아 이동매체에 대한 멀웨어 감염 등 다양한 위험에 노출되어 있다**[3][5]**.

셋째, 제한된 해상통신 환경으로 인해 선내 설치된 운영체계(OS)와 각 장비의 고유한 기능 구현을 위한 운영프로그램에 대한 소프트웨어 업데이트가 원활히 이루어지지 않고 있다. 육상에서는 온라인으로 최신의 OS, 응용프로그램에 대한 패치 파일이 업데이트 되지만, 선박에서는 **Table 1**과 같이 제한된 해상 통신 환경 때문에 소프트웨어 업데이트가 온라인으로 이루어지지 못하고, 선박이 육상에 정박하면 업데이트 파일을 CD, USB 등 이동매체로 전달받아 해당 컴퓨터에 수동으로 설치되고 있다**[5][11]**.

Table 1: Maritime satellite communication system **[11]**

System	Band	Range	Bandwidth	Comment
Inmarsat C	L	A3	9.6kbps, packet oriented	GMDSS, short e-mails
Inmarsat fleet	L	A3	128-450 kbps	GMDSS, supports internet
Iridium	L	A4	134 kbps (open port)	Also coverage in arctic.
VSAT shared link	C, Ku, Ka	A1-A3	Any, typical 64-512 kbps. shared by several users.	Normally not deep sea.
VSAT dedicated link	C, Ku, Ka	A1-A3	Any, dependent on price. dedicated capacity to user.	Coverage varies with system and price.
Other (Orb-comm, ect.)	L, S, C, Ku, Ka	A1-A4	Typically low, usually up to telephone.	Ether bent pipe systems or store and orward.

뿐만 아니라 선박에 탑재된 컴퓨터는 함교(bridge), 엔진룸, 선실 뿐 아니라 장비실과 같이 사람의 접근이 어려운 위치가 많아 수많은 선내 컴퓨터가 안전 패치조차 인스톨하지 않은 상태에서 운영되고 있어 사이버 공격에 대한 대응이 매우 어려운 상황이다**[6][10]**.

넷째, 개인통신에 대한 보안 및 관리 기술이 부재하다. 현재 대부분의 선박에서는 bridge와 일부 업무용 PC에서만 선육간 통신을 허용하고 있지만 일부 해운선사에서는 선원복지를 위해 wi-fi와 인터넷 등 개인 네트워크 환경을 제공하고 있으며, 선원복지, 근무환경 개선 등에 대한 요구로 개인 네트워크 환경에서의 선육간 통신 서비스가 확대되어 가고 있다. 하지만 아직까지 선박은 육상과 같은 보안 인프라가 구축되어 있지 않으며, **Table 1**과 같이 통신 속도와 요금에 많은 제한을 받기 때문에 개인통신 사용량에 대한 통제가 필요하다. 특히 사이버 보안사고 대부분은 인적과

실에 의해 발생되기 때문에 개인 통신 환경에서의 사이버 보안에 대한 대안이 필요하다**[3][5][11]**.

다섯째, 안티바이러스 기술이 부재하여 멀웨어(malware, malicious software)와 같은 악성 소프트웨어나 에드웨어(adware) 등에 대한 위협도 함께 증가하고 있다. 육상에서는 안티바이러스 기술을 필수적으로 사용하고 있으나, 해상의 경우 거의 적용되지 않고 있다. 일부 솔루션을 사용하는 대형 해운선사에서도 선내 장비 업그레이드 방법과 동일하게 항만에 입항 시 안티바이러스의 최신버전을 CD, USB등 이동매체를 이용하여 업데이트하고 있어 진화되고 있는 사이버 위험에 대한 적극적인 대처가 어렵다**[7]-[9]**.

2.2 선박 사이버 보안에 대한 국제동향

이와 같이 다양한 사이버 위험에 노출되어 있는 해운산업의 해상 사이버 보안 대응을 위해 미국과 캐나다는 선박의 보안과 항만 및 해운산업에 대한 자발적 가이드라인 개발에 대한 필요성을 IMO 해사안전위원회(MSC, maritime safety committee) 94차 회의에 제기하였다**[12]**.

MSC 95차 회의에서는 사이버 보안의 범위가 해양산업전체가 아닌 선박에 대한 사이버 보안 지침을 개발하는 것으로 결정되었으며, 발트국제해사협의회(BIMCO; baltic and international maritime council), 국제건화물선주협회(INTERCARGO, international association of dry cargo shipowner), 국제해운회의소(ICS; international chamber of shipping), 국제유조선주협회(INTERTANKO; international association of independent tanker owner), 국제정유사포럼 (OCIMF; the oil companies international marine forum) 등에서 제안된 선박사이버 보안 가이드라인(the guidelines on cyber security onboard ships)이 제시되었다**[13][14]**.

IMO는 MSC 96차 회의에서 해상 사이버리스크 관리에 대한 임시지침(MSC.1/Circ. 1526)을 승인하고 MSC 98차 회의에서 회람서를 승인하였으며, 기국들에게 안전관리시스템에 사이버리스크 관리를 포함하도록 권고하기로 합의하였다**[13][14]**. 이에 따라 ISM 적용 선박은 2021년 1월 1일 이후 사업장의 안전관리적합증서(DoC; document of compliance)의 첫 번째 연차 검사일까지 DoC에 사이버리스크 관리가 포함되도록 권고되고 있다**[15]**.

OCIMF는 TMSA(the tanker management and self assessment)의 효율화 작업의 일환으로 사이버보안을 포함한 항목을 추가하여 TMSA3을 제정하였으며, RIGHTSHIP에서는 사이버보안을 포함한 추가 검사 사항을 반영하여 RIGHT SHIP 검사표를 최신화하였다**[9]**.

또한 ISO/TC80/SC 1에서는 해상에서의 사이버 보안을 위해 해운선사 안전 관리 시스템으로서의 사이버 안전 관리 시스템을 수립, 구현, 유지 및 지속적인 개선을 위한 지침 제정 작업이 이루어지고 있다**[16]**.

3. 선박 사이버 보안 규정 분석

3.1 BIMCO

BIMCO 선박 사이버 보안 가이드라인에서는 사이버 보안을 **Figure 2**와 같이 위험 요소 식별, 식별된 위험에 대한 취약점과 위험 노출 평가, 평가 결과에 대한 보호 방안, 비상 대책 수립, 비상대책에 따른 대응으로 정의하고, 가이드라인의 적용을 받는 선박에 탑재된 잠재적 취약장비를 **Table 2**와 같이 규정하였다**[17]**.

Figure 2: Cyber security awareness as set out in the guideline **[17]**

Table 2: Target system, equipment & technologies of cyber security onboard ships guideline **[17]**

Item	Contents
Communication system	satellite communication, equipment, VoIP equipment, wireless network
Network system	router, switch, fire walls, VLAN, etc.
Control/monitoring system	propulsion and machinery management and poser control system, access control system, cargo management system
Navigation	bridge system(GPS, ECDIS, DPS, AIS, GMDSS, VDR)
Crew system	administratice and crew welfare system (crew wifi, lan internet access)

Table 3: Types of cyber attack **[17]**

Untargeted attack	Targeted attack
• social engineering • phising • water holing • ransomware • scanning	• spear-phishing • deploying bontnets • subverting the supply chain

사이버 공격은 **Table 3**과 같이 피싱, 워터홀링 등 일반적인 기술을 사용하여 불특정 다수의 선사 및 선박의 시스템

과 데이터를 공격하는 무차별 공격과 특정 정보를 캐내기 위한 스피어싱(spear-phishing), 대규모 네트워크 공격을 위한 봇네트 배포(deploying botnets) 등의 방법을 이용하여 선사 및 선박의 특정 시스템 또는 데이터를 공격하는 표적 공격으로 구분한다.

사이버 공격은 조사/정찰(survey/reconnaissance), 전달(delivery), 파괴(breach), 영향(affect)의 4단계로 구분된다.

조사단계에서는 사이버 공격을 위한 방법 수집과 개발, 전달 단계에서는 공격 도구의 배포, 파괴 단계에서는 실질적으로 시스템과 데이터에 대한 공격이 이루어지며, 영향 단계에서는 공격으로 인한 피해가 발생된다.

사이버 보안에 대한 취약점은 선사 또는 선박의 IT (information technology), OT(operation technology) 및 정보와 데이터 적용 현황에 따라 달라지며, 위험 노출도 평가는 CIA (confidentiality, integrity and availability) 모델 프레임워크에 따라 다음의 항목에 대한 3단계 영향을 평가한다.

- 선원, 승무원, 화물 및 승객에 대한 정보나 데이터에 대한 접근
- 사이버 공격으로 선박의 안전 및 운항 효율 관련 자료의 무결성 상실
- 정보 또는 데이터 변조 및 서비스 중단으로 인한 데이터 가용성 상실

선박 사이버 보안 가이드라인에서는 사이버 보안에 대한 대응방안을 선박 보안 담당자나 IT 부서장이 아닌 경영자 선에서 정의될 것을 권고하고 있으며 사이버 보안 위험에 대한 대응 방안으로 **Table 4**와 같이 기술적인 방안과 절차적인 방안을 제시하였다.

Table 4: Cyber security controls **[18]**

Technical cyber security controls	Procedural controls
• control network ports, protocols and services • firewalls, routers etc. • secure configuration for HW and SW • e-mail and web browser protection • satellite and radio communication • malware defences • data recovery capability • wireless access control • software security • secure network design • physical security • boundary defence	• training and awareness • upgrade and software maintance • anti-virus & anti-malware tool updates • use of administrator privileges • physical and removable media controls • equipment disposal, including data destruction • obtaining support from ashore and contingency plans

3.2 영국선급

영국선급(LR, lloyd's register)은 해운산업분야의 사이버 보안을 다룬 CES(cyber-enabled ship) 가이드라인을 발표하였다.

CES 가이드라인은 사이버 시스템 정의, 6가지 위험 영역에 대한 고려사항, CES에 대한 평가방법으로 구성된다**[16]**.

CES 대상 범위는 항해, 기관장비 뿐 아니라 선박에 설치된 센서, 모니터링 시스템, 컨트롤 시스템, 하드웨어와 같은 ICT 장비, 해사데이터, 빅데이터, 위성 및 라디오 통신, VoIP, E-mail 등이 포함된다.

CES 가이드라인은 주요 위험영역을 일반적인 시스템과 5가지 경계로 구분하고 이에 대한 고려사항을 제시하였다.

첫째, 시스템은 산업표준에 따라 구현, 관리되어야 하며 위험기반 접근법에 따라 안정적인 운영과 시스템 복구 기능을 보증해야 한다.

시스템 구현 및 관리에 대한 산업 표준은 ISO/IEC/IEEE 15288(system and software engineering – system lifecycle process)와 ISO/IEC/IEEE 12207(system and software engineering – software lifecycle process)이며, 위험기반접근법은 영국 선급의 ARBD(assessment of risk based design) 기법, NIST(national institute of standards and technology) 표준, SP 800-64(security considerations in the system development life cycle)를 적용할 수 있다.

둘째 휴먼시스템(human-system)은 의존성과 신뢰성을 확보하기 위하여, 시스템 개발 및 운영에 대한 구조화된 HCD (human centred design) 접근이 필요하다.

ICT 기술은 선박의 안전과 운항, 육상 지원업무 등 전통적인 작업을 지원하거나 일부 대체할 수 있으므로 각 장비의 개별적인 사용자 인터페이스가 아닌 선원과 육상직원 모두 안전하고 효율적으로 작업이 가능한 통합 사용자 인터페이스가 필요하다. 통합 사용자 인터페이스 개발은 ISO 9241-210(human centred design for interactive systems)에 따라 휴먼시스템 개발 및 운영에 대한 구조화된 HCD 접근이 필요하다.

셋째, 네트워크 및 통신은 해상표준을 준수해야하며, 우선순위에 따른 통신과 데이터 무결성을 보장해야 한다.

선박 네트워크 및 통신은 해상환경에 적합한 표준을 만족하고 중요한 통신 인프라에 대한 스페어를 확보해야하며, 설치된 시스템에 대한 적절한 유지보수 절차가 필요하다. 뿐만 아니라 비상상황에서 안전 또는 경영 시스템이 우선시 될 수 있도록 사용 가능한 통신 대역폭에 접근할 수 있는 접근성과 편의성을 확보해야 한다.

넷째, 소프트웨어는 국가 표준이나 IEC 61508과 같은 국제 표준을 만족해야하며, ISO 9001 표준에 적합한 생산, 유지보수 등을 보장해야한다.

CES의 소프트웨어 관리 요소는 다음과 같다.

- 소프트웨어 변경에 대한 책임은 자격요건을 가진 엔지니어가 수행하여야 함

- 변경 후 시스템 통합, 통신, 운영 및 유지보수가 신속, 정확하게 운영되어야 함
- 변경 시 선원과 협의하며, 선박의 통제하에 있어야 함
- 변경 사항이 기존과 다르게 보이거나 동작할 경우 변화 관리 계획과 재교육이 제공되어야 함
- 소프트웨어 버전과 매개변수 형식 간의 호환성이 보장되어야 함
- 새로운 버전의 정확한 동작을 보여줘야 함

다섯째, 데이터 신뢰성을 위하여 시스템 설계 단계에서 무결성(integrity), 유효성(availability), 인증(authentication), 비밀(confidentiality), 허가(authorization), 부인방지(non-repudiation)를 고려해야한다.

여섯째, 사이버 보안은 시스템 개발에 미치는 영향뿐 아니라 직원의 교육, 조직문화 등의 사항을 고려해야한다.

LR은 진화되는 새로운 기술을 신속하게 채택할 수 있도록 CES 가이드라인에 **Figure 3**의 프로세스에 따라 특정 시스템을 평가할 수 있는 통합된 위험 기반 접근 방식을 적용한다.

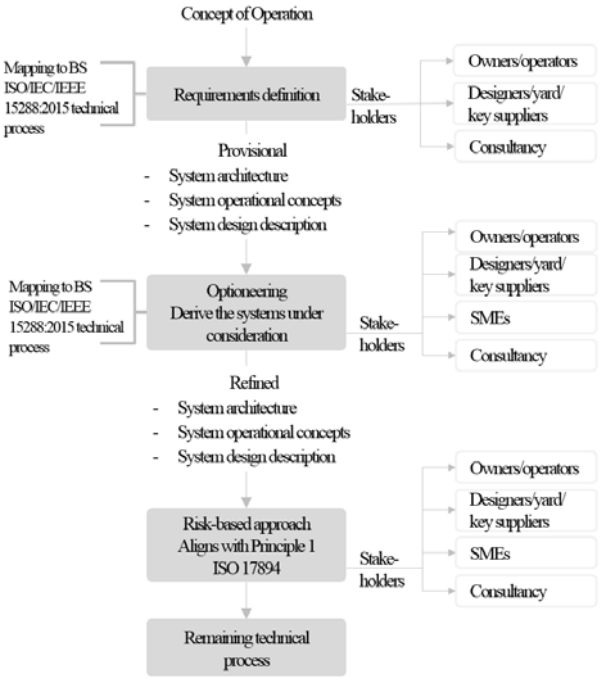

Figure 3: 'phase 1' process map for risk-based appraisal of cyber-enabled system **[18]**

3.3 미국선급

미국선급(ABS, american bureau of shipping)은 ABS CyberSafety™ 시리즈의 일부로서 시스템, 선박 및 플랫폼에 대한 사이버 보안 가이드라인(the application of cybersecurity principles to marine and offshore operations) VOLUME 1 : CYBERSECURITY를 발표하였다**[19]**.

ABS 사이버시큐리티는 모범 사례(best practice)를 통해 선박 및 플랫폼에 대한 사이버 보안 가이드라인을 제시하였다. best practice 구조는 **Figure 4**와 같이 기본 기능 (basic capability), 개발 기능 (developed capability)으로 구성되며, 사례, 프로그램 및 프로세스, 리스크 이해 및 관리, 보호된 리소스 및 접근으로 구분된다.

Figure 4: Structure for best practices **[19]**

기본 기능은 **Figure 4**의 내부 원에 포함된 기본적인 9가지 기능으로 비즈니스 또는 운영 체제를 지원하기 위해 주로 사용되는 정보 기술 기반의 기능이다. 기본 기능은 반드시 조직 내에서 개발, 구현되어야 하며 명확하게 문서화되고, 사용되고, 지원되고, 유지되어야 한다.

개발 기능은 사이버 보안의 기본 기능을 보다 개발적 기능으로 확장하는 방법을 다루며 데이터 보호, 성능 시스템과 보안 시스템의 모니터링, 사고 시 복구 기능 어플리케이션 패치 등에 대한 best practice를 제시하였다.

ABS 사이버시큐리티는 기본 기능, 개발 기능에 대한 best practice외에 엔지니어링 제공, 설계 관리 도구, 투자 통제 실시와 같은 부가 기능에 대한 best practice도 제시하였다.

3.4 OCIMF TMSA & RIGHTSHIP

OCIMF는 유조선 선박 운영자가 안전관리 시스템을 평가, 측정 및 개선하는데 도움이 되는 표준 프레임 워크를 제공하는 유조선 관리 및 자체평가 우수 사례 안내서인 TMSA 3차 개정판을 2017년 4월에 발표하였다**[20]**.

개정된 TMSA 3에는 해상 보안을 다루는 element 13이 포함되어 있으며, 사이버 보안 관련 주요 요구사항은 **Table 5**와 같다.

Inspection and assessment report for dry cargo ship 검사에서는 기존 선박 점검표(FOD06(10))에 **Table 6**의 사이버 보안을 추가한 검사 사항을 반영하여 RIGHTSHIP 점검표를 개정하고, 2017.05.11.부터 검사에 적용하고 있다**[9]**.

Table 5: Cyber security requirements (included in element 13 maritime security) **[20]**

No.	KPI
13.1.2	The company has documented procedures in place to identify security threats applicable to vessels trading areas and shore-based locations.
13.2.3	Policy and procedures include cyber security and provide appropriate guidance and mitigation measures.
13.2.4	The company actively promotes cyber security awareness.
13.3.2	Security procedures are updated taking into account current guidance.
13.4.5	The company is involved in the testing and imple- mentation of innovative security technology and system

Table 6: RIGHTSHIP inspection checklist (cyber security) **[9]**

No.	KPI
4.7.1	Does the vessel and/or company have documented soft- ware/firmware and hardware maintenance procedures?
4.7.1.1	Are service reports available?
4.7.2	Does the vessel and/or company have any cyber security procedures?
4.7.2.1	Has a risk assessment for cyber attack been completed?
4.7.2.2	Is a cyber attack response plan available?
4.7.3.	Does the vessel and/or company provide any cyber security training?

4. 선박 사이버 보안을 위한 기술 제안

산업계와 각 선급에서 발표되고 있는 사이버 보안 가이드라인에는 사이버 보안에 대한 인식의 개선과 이행을 위한 내부 절차, 기술 및 교육이 언급되고 있다.

본 논문에서는 사이버 보안에 대한 인식 개선, 이행 절차, 기술, 교육 중 사이버 보안을 위한 기술을 다루며, 발표된 사이버 보안 가이드라인 중 기술적 요구사항을 구체적으로 제시한 BIMCO의 사이버 보안 가이드라인을 기준으로 한다.

BIMCO는 사이버 보안을 위한 기술적 방법으로 표 4와 같이 네트워크 포트, 프로토콜 및 서비스의 관리, 방화벽, 라우터, 스위치와 같은 네트워크 장비 구성, 하드웨어 및 소프트웨어에 대한 보안 구성, 이메일 및 웹브라우저 보안, 위성 및 라디오 통신에 대한 보호, 멀웨어 방지, 데이터 복구, 무선 엑서스 제어, 어플리케이션 패치 관리, 보안 네트워크 설계, 경계방어 등을 제시하였다. 본 논문에서는 제안된 12가지 기술을 **Figure 5**와 같이 보안이 강화된 네트워크 구성, 선내 통합 네트워크 관리, 데이터 보안, 선박용 안티바이러스 서비스로 구분하고 이에 대한 기술을 제안한다.

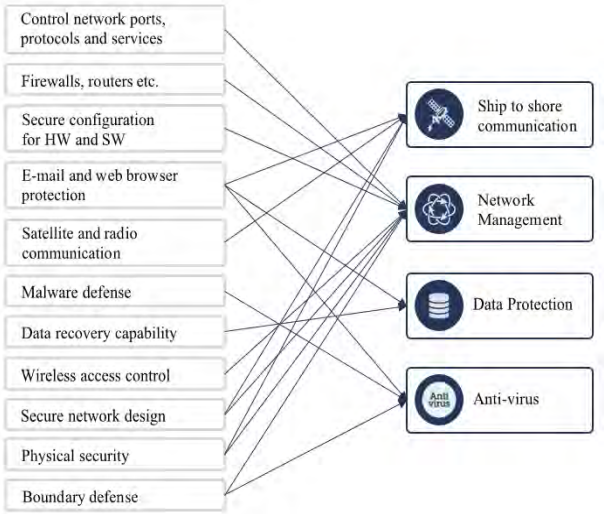

Figure 5: Technical proposal for ship cyber security

4.1 보안이 강화된 네트워크 구성

현재 선박에서는 네트워크의 운용, 설치 편의성을 위해 일부 게이트웨이와 스위치를 사용하여 구역별로 네트워크를 분리하고 업무용 PC와 개인용 PC에 외부 통신을 제한적으로 허용하고 있다. 최근 선박과 육상간 데이터 공유와 개인 통신에 대한 요구가 증가하고 있어 외부 통신에 대한 개방이 필요하지만 현재 선박에 설치된 일부 게이트웨이와 스위치만으로는 사이버 보안에 대한 대응이 어려워 보다 강화된 네트워크 구성이 필요하다.

대부분의 사이버 보안 사고는 사용자 또는 시스템이 권한 밖의 시스템 또는 데이터를 사용하여 발생되기 때문에 운영 목적에 따라 네트워크를 구성하고 접근 권한을 부여하며 VPN, 방화벽과 같은 보안 장비를 운영하여야 한다.

MiTS(maritime information technology standard)에서 제안한 **Figure 6**의 선육간 네트워크 구성과 같이 주요 네트워크와 시스템을 식별하여 한 네트워크에서 사이버 사고가 발생되어도 다른 네트워크에 영향을 미치지 않도록 선내 네트워크를 구성하여야 한다**[21]**.

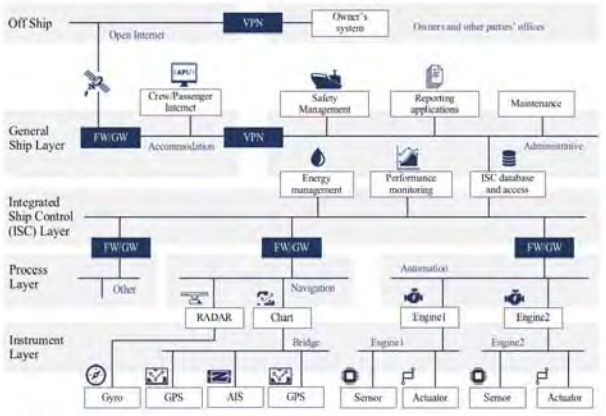

Figure 6: Networks on board and shore **[21]**

구분된 네트워크에 시스템 접근 권한을 정의하고, 각 네트워크 영역과 노드 사이에 방화벽, 게이트웨이 등을 설치함으로서 외부의 사이버 공격에 대비할 수 있다. 특히 외부 통신 구간에 VPN을 설치하면 VPN 장비의 인증을 거친 후 선내 시스템에 접속할 수 있으며, 네트워크 트래픽이 암호화되어 방화벽을 통한 서비스 통제, 접근 대상 서비스 인증을 거치므로 보다 높은 보안 수준을 가진 선내 네트워크를 구성할 수 있다.

4.2 통합 네크워크 관리

4.2.1 위성포트 및 네트워크 상태 모니터링

앞서 기술된 바와 같이 대부분의 사이버 보안 사고는 사용자 또는 시스템이 권한 밖의 시스템 또는 데이터를 사용하여 발생되기 때문에 선육간 통신 구간에 대한 모니터링을 통해 사이버 공격을 감지할 수 있지만 현재 선박에는 이러한 시스템이 부재하여 사이버 공격에 대한 신속한 대응이 어려운 상황이다.

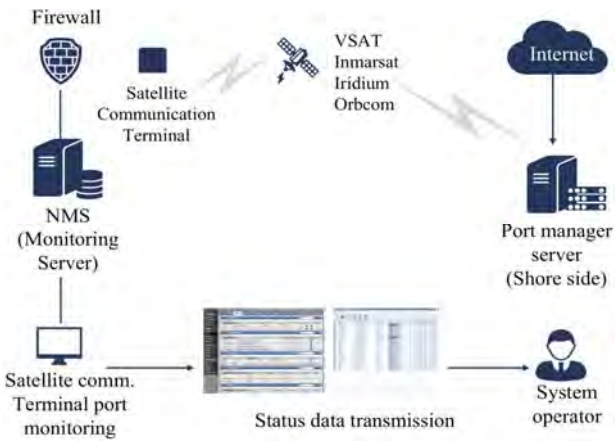

Figure 7: Satellite port monitoring configuration diagram

Figure 7과 같이 위성포트를 모니터링하면 인가되지 않은 포트의 연결과 비정상적인 통신 패턴 및 권한 밖의 사용자 또는 시스템 접근을 실시간으로 확인하여 선육간 통신 구간에서의 사이버 공격/위험을 감지할 수 있다.

또한 선내에 설치된 방화벽, 게이트웨이, 무선 AP(access point)를 연동하여 외부 침입, 내부 위험 감지 등을 확인하며 위험감지 시 해당 네트워크 및 노드의 방화벽, 게이트웨이, AP를 제어함으로서 다른 네트워크로의 2차 피해를 방지할 수 있다.

4.2.2 보안이 적용된 선박용 웹브라우저

2006년 해사노동협약의 발효(2013)로 인해 선박 환경 및 선원복지환경 개선요구가 증가하고 있으며, 스마트 기기의 대중화에 따른 인터넷기반 유무선 통합기술의 수요와 선원 개인 통신에 대란 요구가 꾸준히 증가하고 있다. 이에 따라 일부 대형 해운선사에서는 선원 거주공간에서의 개인 네트워크 환경을 제공하고 있다. 사이버 보안 사고의 원인은 인적과실, 특히 웹서비스를 이용하는 과정에서 발생되는 경우가 가장 많기 때문에 웹서비스 환경에서의 개인 통신환경에 대한 보안 기술이 필요하다.

현재 선박에서 사용되고 있는 웹서비스 제공 방법은 **Figure 8**과 같이 사용자가 파일, 연결, 웹 페이지 등과 같은 자원을 프록시 서버에 요청하면 프록시 서버는 웹사이트와 클라이언트사이에서 대신 통신을 수행하며, 원격에 요청된 자원을 캐시하여 자원 재 요청 시 프록시 서버 내 정보를 제공하고 있어 보안에 취약한 단점이 있다.

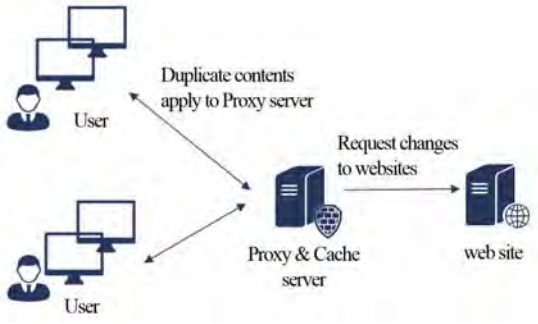

Figure 8: Typical proxy & cache server configuration

이러한 단점을 보완하기 위하여 **Figure 9**와 같은 프록시 서버를 육상시스템에 구성하여 IP, 사용자, 도메인 등에 대한 필터링 정책을 관리하고 사용자 계정을 생성하여 개인 통신 환경을 관리하며, 해운선사에서 지정한 필터링 정책에 따라 웹사이트의 멀티미디어 데이터를 필터링하고 텍스트와 이미지를 압축함으로서 경제적이고 보안이 강화된 개인통신환경을 제공할 수 있다.

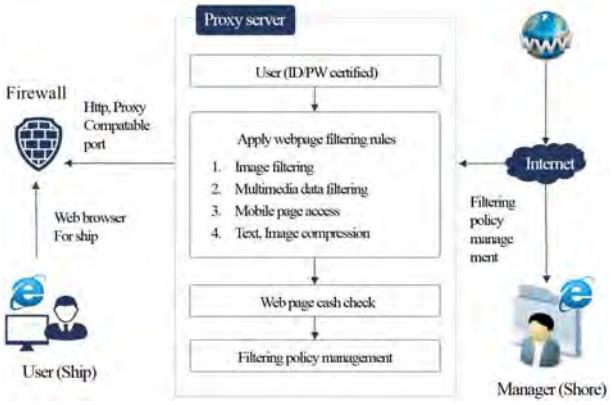

Figure 9: Secure web browser for ships

4.2.3 SNMP 기반 IP 장비 모니터링

최근 선박 장비의 IT화, 네트워크화되면서 다양한 기능과 편의를 제공하는 반면, IT 기술의 고도화와 개별적으로 운영되는 장비수 증가로 인해 제한된 인원과 IT 전문지식이 부족하여 외부 공격에 대한 모니터링과 사고발생 시 신

속한 대응이 어려운 단점이 있다.

선내 설치된 다양한 IP 장비의 운용, 설정과 MS 운영체계를 사용하는 선내 컴퓨터를 **Figure 10**과 같이 선내 각 네트워크 영역과 노드 사이에 설치된 방화벽, 게이트웨이와 각 네트워크에 설치된 IP 기반의 모든 장비, 컴퓨터를 SNMP(simple network management system)기반으로 모니터링하고 제어할 수 있다.

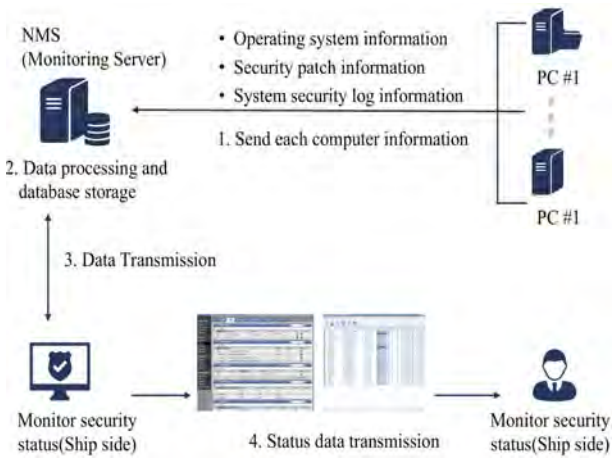

Figure 10: Monitoring of IP equipment

SNMP를 이용하여 TCP/IP 기반의 네트워크에서 정기적으로 네트워크상의 각 IP 장비에 대한 여러 가지 정보를 수집하여 IP 장비의 상태를 모니터링 할 수 있으며, IP 장비 또는 네트워크에 비인가장치의 연결을 실시간으로 확인하여 비인가 장비의 접속으로 발생되는 위험을 예방할 수 있다. 또한 IP 장비의 OS 버전, 보안 상태 및 응용 프로그램의 버전을 확인하고 육상에서 최신의 업데이트 파일을 받아 업데이트가 필요한 IP 장비에 자동업데이트 함으로써 사람의 접근이 어려운 곳에 설시된 IP 장비도 OS, 보안 패치 등을 효율적으로 관리할 수 있다.

4.3 데이터 보안

선내 수집 데이터를 활용하는 선박 및 육상 어플리케이션과 서비스가 증가하면서 선내 및 선육간 네트워크 통신 구간에서 데이터 보안의 중요성이 강조되고 있지만 선내, 선박과 육상간 데이터 통신 구간에서 해사데이터에 대한 보안이 부재하다.

선박과 육상간 데이터 통신구간에서 데이터 보안을 위해서는 해사데이터를 암호화하고 통신구간에 SSL(secure sockets layer)과 같은 보안 기술을 적용할 수 있다. SSL은 사이버 공간에서 전달되는 정보의 안전한 거래를 보장하기 위한 인터넷 통신규약 프로토콜으로, 해사 데이터에 SSL을 적용하여 서버와 클라이언트의 진위 확인, 암호화키와 관련된 협상, 상위 응용프로그램이 정보를 서버와 교환하기 전에 서버의 진위를 확인함으로서 해사 데이터의 보안을 확보할 수 있다.

4.4 선박 안티바이러스 서비스

대부분의 선박에는 보안 관련 소프트웨어가 설치되지 않고 OS 업데이트가 이루어지지 않고 있어 바이러스 감염에 쉽게 노출되어 있으며, 시스템 호환 등과 같은 문제가 발생되고 있다. 이러한 문제점은 발표된 여러 해상 사이버 보안 가이드라인에도 명시되어 있어 선박용 안티바이러스 기술의 적용이 반드시 필요하다.

해상통신환경은 육상과 달리 통신 사용량과 대역폭이 제한되기 때문에 육상에서와 같은 방법으로 바이러스 패치를 업데이트할 수 없다. 따라서 선박용 안티바이러스 서비스는 **Figure 11**과 같이 육상에서는 안티바이러스 제조사로부터 최신 업데이트 파일을 수신하여 기존 파일에서 추가된 최신의 패치 파일만 선별하여 선박으로 전송한다. 선박에서는 최신 업데이트 패치 파일을 수신하여 안티바이러스 제조사와 업데이트 패턴을 공유함으로써 경제적인 방법으로 선박에 안티바이러스 서비스를 제공할 수 있다.

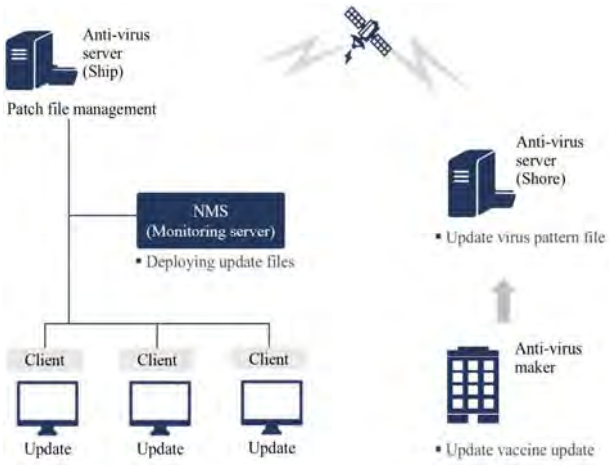

Figure 11: Configuring antivirus service for ship

5. 결 론

본 연구에서는 선박 사이버 보안에 대한 기술을 분석하고 사이버 보안에 대한 기술적 구현 방안을 다음과 같이 제시하였다.

첫째, 선박 사이버 보안에 대한 기술현황을 분석하고 BIMCO와 영국, 미국 선급에서 발표된 사이버 보안 가이드라인을 분석하였다.

둘째, 선박 사이버 보안 가이드라인에서 제시한 사이버 보안을 위한 12가지 기술적 방법을 보안이 강화된 네트워크 구성, 통합 네트워크 관리, 데이터 보안, 선박 안티바이러스 서비스의 4가지로 구분하고 이에 대한 기술을 제안하였다.

앞으로 수행될 연구에서는 제안된 기술을 구현하고 선박 사이버 보안에서 제시한 이행 절차를 시스템화 하여 선박 사이버 보안에 대한 기술개발을 완료하고자 한다.

후 기

본 연구는 2017년도 국가표준기술력향상사업(선박 안전관리 및 정비용 소프트웨어 기반 PMS 시스템 국제 표준화 연구개발)의 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

References

[1] D. K. Moon, J. Y. Bae, J. H. Park, K. I, Lee, and H. B. Kim, “A development of remote ship maintenance system based on ship area network,” Journal of the Society of Naval Architects of Korea, vol. 47, no. 5, pp. 751-756, 2010 (in Korean).

[2] S. M. Mun and J. Y. Son, “Current activities of navogation & communication equipments industry and R&D,” Journal of the Korean Society of Marine Engineering, vol. 35, vol. 4, pp. 512-518, 2011 (in Korean).

[3] Anne Moschner, CMA Shipping 2015: DNV GL addresses cybersecurity risks, 2015. [Internet]. Available: http://www.safety4sea.com/cyber-security-threats-and-risks/, Accessed August 14, 2017.

[4] S. M. Mun, W. S. Jang, and J. Y. Son, “An Information exchange software supporting nultiple media communication in vessels,” Journal of the Korean Society of Marine Engineering, vol. 35, no. 5, pp. 647-653, 2011 (in Korean).

[5] Monthly Maritime Korea, New Challenge for Global Shipping ‘Cyber Security’, 2015. [Internet]. http://m.monthlymaritimekorea.com/news/articleView.html?idxno=17008, Accessed August 14, 2017.

[6] H. F. Willan, Cyber Security for Shipping, 2015. [Internet]. Available: http://www.lexology.com/library/detail.aspx?g=e65a5e48-8c49-4e12-b67e-0a469b3b9bed, Accessed June 30, 2017.

[7] J. Leyden, Major Cyber Attack Hits Norwegian Oil Industry, 2014. [Internet]. Available: https://www.theregister.co.uk/2014/08/27/nowegian_oil_hack_campaign/, Accessed May 4, 2017.

[8] Korea Shipping Gazette, ‘Digital armed poart logistics industry ransomware become a target’, 2018. [Internet]. http://www.ksg.co.kr/news/main_newsView.jsp?page=2&bbsID=news&schVal=%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4&categoryCode=search&bbsCategory=KSG&pNum=114508&backUrl=news_search, Accessed August 30, 2017.

[9] KOREA P&I, Guidelines for Cyber Security in TMSA, RIGHTSHIP and ISM, 2018. [Internet]. http://www.kpiclub.or.kr/board/bbs/board.php?bo_table=News_03&wr_id=355, Accessed August 30, 2017.

[10] BIMCO, “Development of cyber security guidelines for the shipping industry,” Big Data in Shipping and Cyber Security Workshop, pp. 7-21, 2015.

[11] O. S. Park and D. H. Kim, “Technical trends in maritime radio communications for e-Navigation,” Electronics and telecommunications trends, vol. 27, no. 2, pp. 51-58, 2012.

[12] IMO MSC 94 Overview and Summary Report, [Internet] https://www1.veristar.com/veristar/dps_info.nsf/0/1dcd319f33ca9fc2c1257da4003d7d3b/$FILE/MSC94%20Report_Polar%20Code.pdf, Accessed July 4, 2017.

[13] IMO report, IFSMA, [Internet] https://www.ifsma.org/IMO_Reports_files/07d9bcf4d92d0a4e86ea280f8c5a2d81-8.html, Accessed July 4, 2017.

[14] Breaking news of IMO MSC96, Class NK, 2016. [Internet] https://www.classnk.or.jp/hp/pdf/info_service/imo_and_iacs/msc96_sum_rev0_k.pdf., Accessed June 9, 2017.

[15] ISM-cyber security, Shipownersclub, pp. 1. Aug. 2017 [Internet] https://www.shipownersclub.com/media/2017/08/ISM-Cyber-security_0817.pdf, Accessed June 9, 2017.

[16] Draft Working Paper on Cyber Safety Management, ISO/ TC 8/SC 1, pp. 1-13, May, 2017.

[17] The Guidelines on Cyber Security onboard Ships, BIMCO, pp. 1-32, February, 2016.

[18] Cyber-Enabledships-aLloyd’s Register Guidancenote, Lloyd’s register, pp. 1-22, February, 2016.

[19] The Application of Cybersecurity Principles to Marine and Offshore Operations, vol. 1, Cybersecurity, American Bureau of shipping, pp. 1-29, February, 2016.

[20] Maunch of the 3rd edition of TMSA, Apr. 2017. [Internet] https://intertanko.com/upload/109531/3%20INTERTANKO%20vetting%20committee%20Athens%20April%202017%20-%20OCIMF.PDF, Accessed May 16, 2017.

[21] Maritime Information Technology Standards, MARINTEK, Aug. 2012 [Internet] http://www.mits-forum.org/network.html, Accessed April 21, 2017.