한국해사포럼

선박 사이버보안 국제 규제동향과 국내 선사의 준비현황

2025.10.24

한국선급 전기자동화팀

유진호 책임검사원

CONTENT

I. 선박 사이버보안의 국제 규제 동향

해사 사이버보안 국제 동향

1. IMO 및 주관청

2017 MSC-FAL.1/Circ.3 - GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.

2017 Res. MSC.428(98)* - MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS.

* Over 24 flag states like USCG, Marshall Island, Singapore, Australia, Cyprus, Vanuatu require it as mandatory.

2020 USCG CVC-WI-027(1) - Vessel Cyber Risk Management Work Instruction

2024 USCG NVIC 02-24 – Reporting breaches of security, …

2023 Cyber Security Code of Practice for Ships Ver.3

2023 Guidelines on Maritime Cyber Safety Management

2024 Enhancement of Maritime Cyber Safety Management

2. 선주 협회

2016 Guidelines on Cyber Security Onboard Ships

2017, 2018. 2nd and 3rd Version of Guidelines on Cyber Security Onboard Ships .

2020 4th Version of Guidelines on Cyber Security Onboard Ships

2019 Implementation Guide for Cyber Security on Vessels v1.0.

3. 화주

2017 TMSA 3 13 Maritime Security 1.2, 2.3, 2.4, 3.2 and 4.5

2018 SIRE VIQ 7 7 Cyber Security 7.14, 15, 16 and 17

2022 SIRE 2.0 7.5 Cyber Security

2017 Inspection and Assessment Report for Dry Cargo Ships 4.7 Cybersecurity

2021 Inspection Ship Questionnaire (RISQ) 12 Security 12.2, 12.7 and 12.8

4. 국제 선급

2018 Cyber Security Rec.153~164

2020 Rec.166 – Recommendation on Cyber Resilience

2022 UR E26 – Cyber Resilience of Ships

UR E27 – Cyber Resilience of onboard systems and equipment

2020 Guidance for Maritime Cybersecurity System

2020 Guidance for Type Approval of Maritime Cyber Security

IMO : International Maritime Organization, USCG : US Coast Guard, BIMCO : Baltic and International Maritime Council, DCSA : Digital Container Shipping Association, OCIMF : Oil Companies International Marine Forum , IACS : International Association of Classification Societies

IMO 사이버 리스크 관리 가이드라인 및 결의서

MSC-FAL.1/Circ.3

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

- **사이버 리스크 위협 및 취약성에 대한 인식을 제고**하기 위한 긴급한 요구에 의해 개발됨
- 현재 그리고 새롭게 등장하는 사이버 위협 및 취약성으로부터 해운을 보호하기 위한 **높은 수준의 권고 사항**
- **5가지 기능 요구사항 : 식별, 보호, 탐지, 대응 및 복구**

Resolution MSC.428(98)

결의서는 2021년 1월 1일 이후 도래하는 첫 회사 Document of Compliance 연차 심사 전에 **사이버 리스크가** (ISM Code**에 정의된**) **안전관리체계에서 적절하게 관리**하도록 주관청에게 권고함.

⇩

IMO에서는 선박에 대한 사이버리스크 관리에 대하여 지속적인 관심을 표하고 있어 현재 Resolution MSC.428(98)에 대해 각 국에서 이에 따르는 것을 비강제적으로 권고하고 있지만, 향후 강제 요건으로 발전할 가능성이 높음.

현재 미국, 마샬 아일랜드, 싱가포르, 호주, 사이프러스, 바누아투 등 22개국에서 강제 요건으로 적용 중임.

I. 선박 사이버보안의 국제 규제 동향

국제해사기구(IMO) 및 주관청

IMO MSC-FAL.1/Circ.3/Rev.3

관리

- 위험 관리 전략, 기대치 및 정책 수립 및 모니터링
- 사이버 위험 관리를 위한 직원 역할과 책임 정의
- 백업 관리 및 재해 복구, 위기 관리와 같은 비즈니스 연속성 보장
  - **담당자 지정, 권한 부여 및 지원**

식별

- 선내 시스템, 사람, 자산, 데이터 및 기능에 대한 사이버 보안 위험을 관리하기 위한 조직적 이해 개발
  - **자산 식별, 자산 목록 작성**, 위협, 취약성 식별을 포함한 **리스크 평가 수행**

보호

- 사이버 사고로부터 선박을 보호하고 선박 운항의 연속성을 최대화하기 위한 적절한 보호 장치 개발 및 구현
  - **계정 보안, 비밀번호 정책, 다중 인증, 망분리, 방화벽, 암호화 정책, 비인가 USB 사용 제한, OT 담당자 교육 등**

탐지

- 선내 사이버 사고의 발생을 탐지하고 식별하기 위한 적절한 조치 개발 및 구현
  - **사이버 위협 및 행위자 전술, 기술 및 절차에 대한 문서화된 목록 유지, 시스템 모니터링**

대응

- 선내에서 탐지된 사이버 사고에 대한 조치를 취하기 위한 적절한 조치 및 활동을 개발 및 구현
  - **사고 보고, 사이버 사고 기록 유지, 사고 대응 교육**

복구

- 사이버 사고로 인해 손상된 선박 운항에 필요한 모든 기능 또는 서비스를 복구하기 위한 적절한 조치 및 활동을 개발 및 구현
  - **사이버 사고 복구 계획서, 복구 교육, 사고 재발 방지 분석**

USCG CVC-WI-027(3)

USCG Office of Commercial Vessel Compliance (CG-CVC)
Mission Management System (MMS) Work Instruction (WI)

Category	Commercial Vessel Compliance (Domestic and Foreign Vessels)				
Title	Vessel Cyber Risk Management Work Instruction				
Serial	CVC-WI-027(3)	Orig. Date	27OCT20	Rev. Date	11OCT23
Disclaimer:	This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is not intended to nor does it impose legally binding requirements on any part. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements. You can use an alternative approach for complying with these requirements if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach (you are not required to do so), you may contact the Coast Guard Office of Commercial Vessel Compliance (CG-CVC) at CG-CVC@uscg.mil who is responsible for implementing this guidance.				
References:	(a) Maritime Safety Committee Resolution 428(98), "Maritime Cyber Risk Management in Safety Management Systems" (b) U.S. Coast Guard Cyber Strategic Outlook, August 2021 (c) International Safety Management (ISM) Code (d) U.S. Flag Interpretations on the ISM Code, (CVC-WI-004(2)) (e) Title 33 Code of Federal Regulations (CFR) Part 96 (f) Chapter IX, Management of the Safe Operation of Ships, International Convention for the Safety of Life at Sea (SOLAS), 1974 (g) Title 33 Code of Federal Regulations (CFR) Subchapter H (h) National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework 2.0, August 08, 2023 (i) Navigation and Vessel Inspection Circular (NVIC) 04-05: "Port State Control Guidelines for the Enforcement of Management for the Safe Operation of Ships (ISM Code)" (j) "Guidelines for Port State Control Officers on the International Safety Management (ISM) Code," MSC-MEPC.4/Circ.4 (k) USCG Oversight of Safety Management Systems on U.S Flag Vessels, (CVC-WI-003(series)) (l) Maritime Safety Committee / Facilitation Committee Circular 3 "Guidelines on Maritime Cyber Risk Management," MSC-FAL.1/Circ.3 (m) USCG Assistant Commandant for Prevention Policy (CG-5P) Policy Letter 08-16 "Reporting Suspicious Activity and Breaches of Security" (n) National Institute of Standards and Technology (NIST), Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, SP 800-160 Vol. 2 Rev. 1, December 2021				

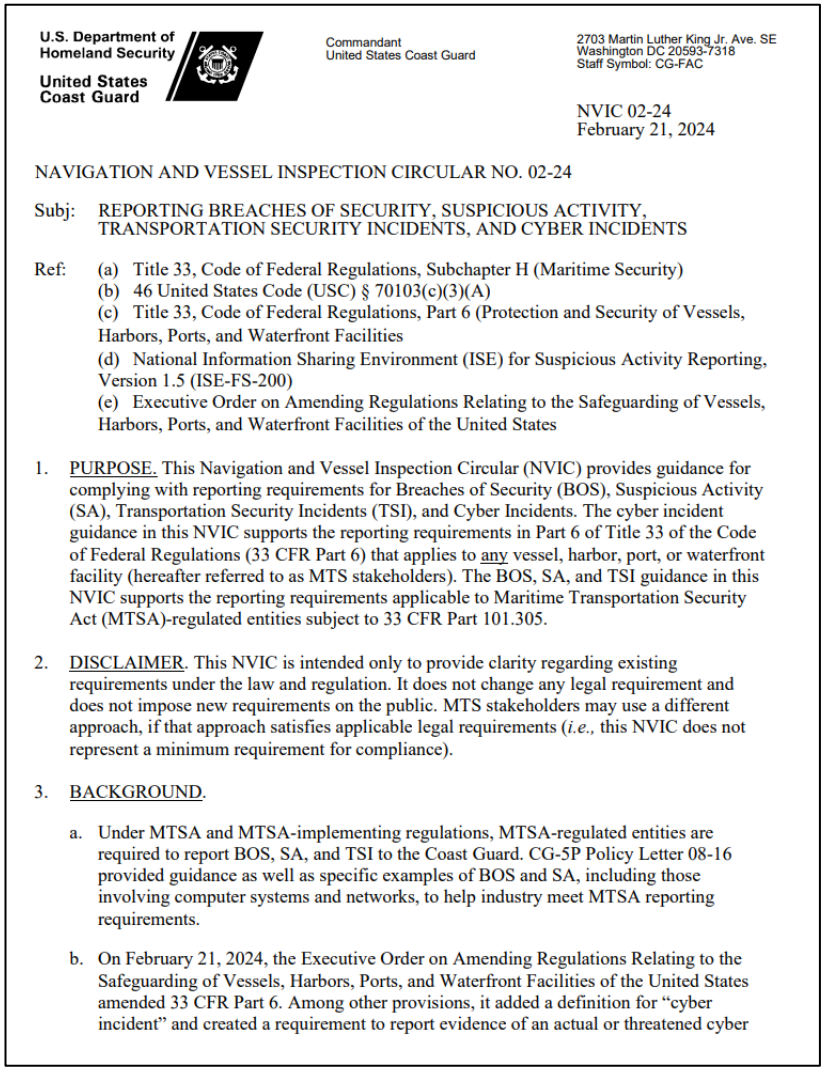
1. **해양 조사관/항만국 통제관은 안전관리체계에 사이버 리스크 관리가 통합되어 있고, 다음의 기본적인 사이버보안을 구현했는지를 확인함.**
   a) 사이버 관행 불량
   - 계정 및 비밀번호 공개 여부
   - 컴퓨터 시스템에 대한 일반적인 로그인 또는 로그인 없는 접속 여부
   - 30분 동안 사용자의 활동이 없을 경우 컴퓨터 기반 시스템의 자동 로그아웃 기능 활성화 여부
   - Flash drive/USB 의 무분별한 사용, 랜섬웨어/과도한 팝업으로 인한 선내 컴퓨터 손상

   b) 사관/선원의 선박 시스템에 영향을 미치는 비정상적인 네트워크 문제와 신뢰성에 대한 불평

   c) 유닛/선박 스크리너가 선장/선원으로부터 잠재적인 스푸핑 이메일을 받음

2. **기술적 운영 관련 결함으로 인한 확대 조사에서 사이버 리스크 관리가 안전관리체계에 통합되어 있지 않은 경우 출항 전 외부 심사 완료와 함께 Code 17 (출항 전 수리) 발행, 확대 조사에서 사이버 리스크 관리가 잘 구현되지 않은 경우 ISM 결함과 Code 40 (다음 입항 전 결함 수정) 또는 Code 50 (30일 이내 결함 수정과 내부 심사 요구) 발행, 사이버보안 사고를 초래한 심각한 결함이 발견되는 경우 ISM 결함과 Code 30 (외부 심사 요구와 출항 정지)**

USCG NVIC 02-24



U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave. SE
Washington DC 20593-7318
Staff Symbol: CG-FAC

NVIC 02-24
February 21, 2024

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-24

Subj: REPORTING BREACHES OF SECURITY, SUSPICIOUS ACTIVITY, TRANSPORTATION SECURITY INCIDENTS, AND CYBER INCIDENTS

Ref: (a) Title 33, Code of Federal Regulations, Subchapter H (Maritime Security)
(b) 46 United States Code (USC) § 70103(c)(3)(A)
(c) Title 33, Code of Federal Regulations, Part 6 (Protection and Security of Vessels, Harbors, Ports, and Waterfront Facilities
(d) National Information Sharing Environment (ISE) for Suspicious Activity Reporting, Version 1.5 (ISE-FS-200)
(e) Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States

1. PURPOSE. This Navigation and Vessel Inspection Circular (NVIC) provides guidance for complying with reporting requirements for Breaches of Security (BOS), Suspicious Activity (SA), Transportation Security Incidents (TSI), and Cyber Incidents. The cyber incident guidance in this NVIC supports the reporting requirements in Part 6 of Title 33 of the Code of Federal Regulations (33 CFR Part 6) that applies to any vessel, harbor, port, or waterfront facility (hereafter referred to as MTS stakeholders). The BOS, SA, and TSI guidance in this NVIC supports the reporting requirements applicable to Maritime Transportation Security Act (MTSA)-regulated entities subject to 33 CFR Part 101.305.

2. DISCLAIMER. This NVIC is intended only to provide clarity regarding existing requirements under the law and regulation. It does not change any legal requirement and does not impose new requirements on the public. MTS stakeholders may use a different approach, if that approach satisfies applicable legal requirements (*i.e.,* this NVIC does not represent a minimum requirement for compliance).

3. BACKGROUND.

a. Under MTSA and MTSA-implementing regulations, MTSA-regulated entities are required to report BOS, SA, and TSI to the Coast Guard. CG-5P Policy Letter 08-16 provided guidance as well as specific examples of BOS and SA, including those involving computer systems and networks, to help industry meet MTSA reporting requirements.

b. On February 21, 2024, the Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States amended 33 CFR Part 6. Among other provisions, it added a definition for "cyber incident" and created a requirement to report evidence of an actual or threatened cyber

1. 보안 위반, 의심스러운 활동, 교통 보안 사고 및 사이버 사고에 대한 요구사항 준수 지침 제공

2. 사이버 사고 보고

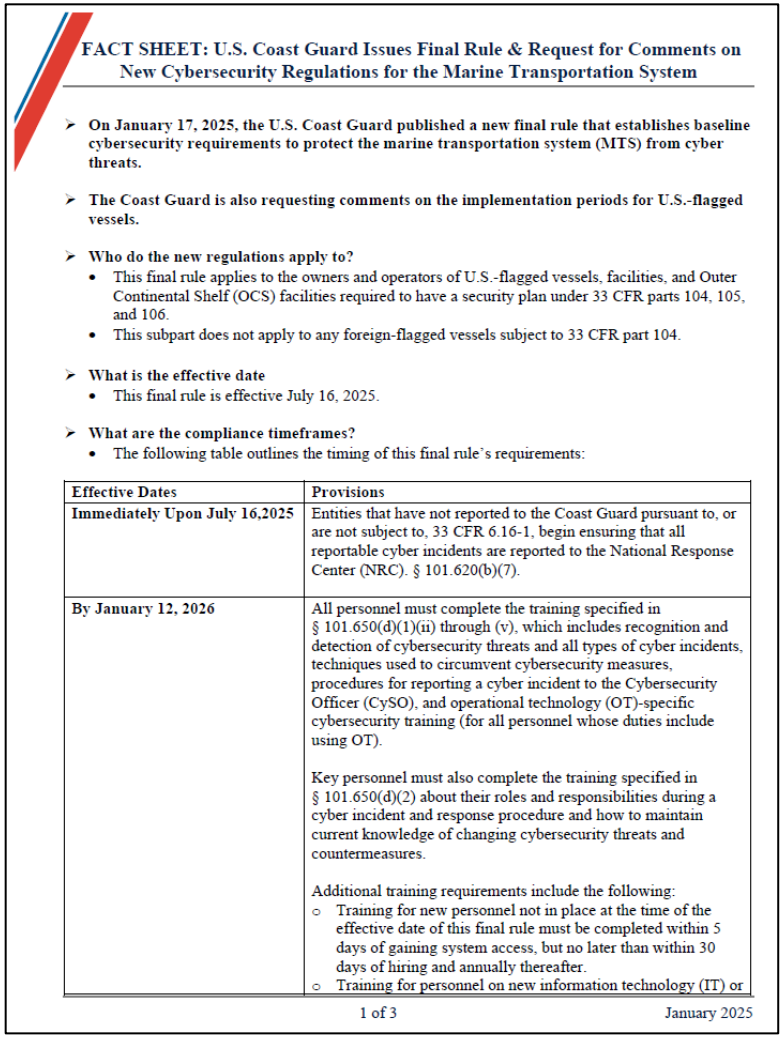
a) 대상 : 모든 선박, 항구, 항만 또는 해안 시설에 적용

b) 사고 정의 : **합법적인 권한 없이 정보나 정보 시스템의 무결성, 기밀성 또는 가용성을 실제로 또는 즉각적으로 위험에 빠뜨리는 사건; 또는 법률, 보안 정책, 보안 절차 또는 허용 가능한 사용 정책을 위반하거나 위반할 임박한 위협**

c) 보고 대상 : 시스템 방어를 침해하지 않는 일상적인 스팸, 피싱 시도 및 기타 성가신 이벤트는 사이버 사고로 보고될 필요 없을 수 있음. 실수로 허용 가능한 사용 정책 위반도 사고에 포함되지 않음.

d) 보고 기관 : 선박, 항구, 항만, 수변 시설에 관한 보호 및 보안법에 따라 **국가대응센터**에 보고하는 것을 추천

Final Rule: Cybersecurity in the Marine Transportation System



FACT SHEET: U.S. Coast Guard Issues Final Rule & Request for Comments on New Cybersecurity Regulations for the Marine Transportation System

- **On January 17, 2025, the U.S. Coast Guard published a new final rule that establishes baseline cybersecurity requirements to protect the marine transportation system (MTS) from cyber threats.**
- **The Coast Guard is also requesting comments on the implementation periods for U.S.-flagged vessels.**
- **Who do the new regulations apply to?**
  - This final rule applies to the owners and operators of U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) facilities required to have a security plan under 33 CFR parts 104, 105, and 106.
  - This subpart does not apply to any foreign-flagged vessels subject to 33 CFR part 104.
- **What is the effective date**
  - This final rule is effective July 16, 2025.
- **What are the compliance timeframes?**
  - The following table outlines the timing of this final rule's requirements:

Effective Dates	Provisions
Immediately Upon July 16,2025	Entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16-1, begin ensuring that all reportable cyber incidents are reported to the National Response Center (NRC). § 101.620(b)(7).
By January 12, 2026	All personnel must complete the training specified in § 101.650(d)(1)(ii) through (v), which includes recognition and detection of cybersecurity threats and all types of cyber incidents, techniques used to circumvent cybersecurity measures, procedures for reporting a cyber incident to the Cybersecurity Officer (CySO), and operational technology (OT)-specific cybersecurity training (for all personnel whose duties include using OT). Key personnel must also complete the training specified in § 101.650(d)(2) about their roles and responsibilities during a cyber incident and response procedure and how to maintain current knowledge of changing cybersecurity threats and countermeasures. Additional training requirements include the following: ○ Training for new personnel not in place at the time of the effective date of this final rule must be completed within 5 days of gaining system access, but no later than within 30 days of hiring and annually thereafter. ○ Training for personnel on new information technology (IT) or

1 of 3 January 2025

1. 2025.1 미국 해상교통시스템에 대한 신규 사이버보안 규정 발표

2. 요약

1) 대상 : **미국적 선박 보유 선주 & 선박관리사, 항만 또는 외대륙붕 시설에 적용**

2) 적용 시점 별 요구 사항

a) 25.07.01 : 33 CFR 6.16-1에 따라 USCG에 신고하지 않았거나 신고 대상이 아닌 기관들은 신고 가능한 모든 사이버 사건이 국가 대응 센터에 보고

b) ~26.01.12 : **모든 직원 및 주요 인력들은 매년 명시된 교육 이수**(사고 대응, OT 보안 등)

c) ~27.07.16 : 선주와 선박관리사들의 **사이버보안 담당자(CySO) 지정, 사이버보안 평가 매년 수행, USCG에 사이버보안 계획서 제출 및 승인 획득**

d) 사이버보안 계획서 승인 후 : **매년 사이버보안 훈련(drill) 최소 2회, 연습(exercise) 최소 1회. 요청 시 계획서 내 사이버보안 부분 및 침투테스트 결과를 USCG에 제출**

해양수산부 선박 사이버안전 강화 관리 지침

해양수산부 | 보도자료 | 당시 대한민국! 세종 국민의 나라

보도일시 (인터넷) 2023. 4. 21.(금) 06:00, (지면) 2023. 4. 21.(금) 석간 | 배포 2023. 4. 20.(목) 14:00

선박 사이버안전 강화 위한 관리지침 제정

- 사이버안전 관리체계 구축 시 해운선사가 고려할 사항과 이를 지원하기 위한 정부의 역할 등 규정
- 4월 말 업·단체 대상 권역별(서울·부산) 설명회 개최 및 10월까지 '해사 사이버안전 종합대책' 수립 예정

해양수산부(장관 조승환)는 교통분야 최초로 정부·민간의 역할을 규정하는 「해사 사이버안전 관리지침(고시)」을 제정하여 4월 21일(금) 시행한다.

이번 고시는 선박을 대상으로 벌어질 수 있는 사이버 공격·위협으로부터의 안전을 확보하고 해운선사를 지원하기 위한 정부의 역할*과 함께, 해운선사가 사이버안전 관리체계를 구축할 때 고려해야 하는 사항**을 권고 성격으로 규정하고 있다.

* △해사 사이버안전 대책 수립·시행, △전문인력 양성, △교육·훈련, △전략·기술 연구개발·보급, △선박·사업장 진단·실태평가, △시스템 취약요소 발굴·개선 등 지원

** △관리조직, △자산관리, △업무분장, △위험성 평가, △보호·탐지·대응·복구 조치 등

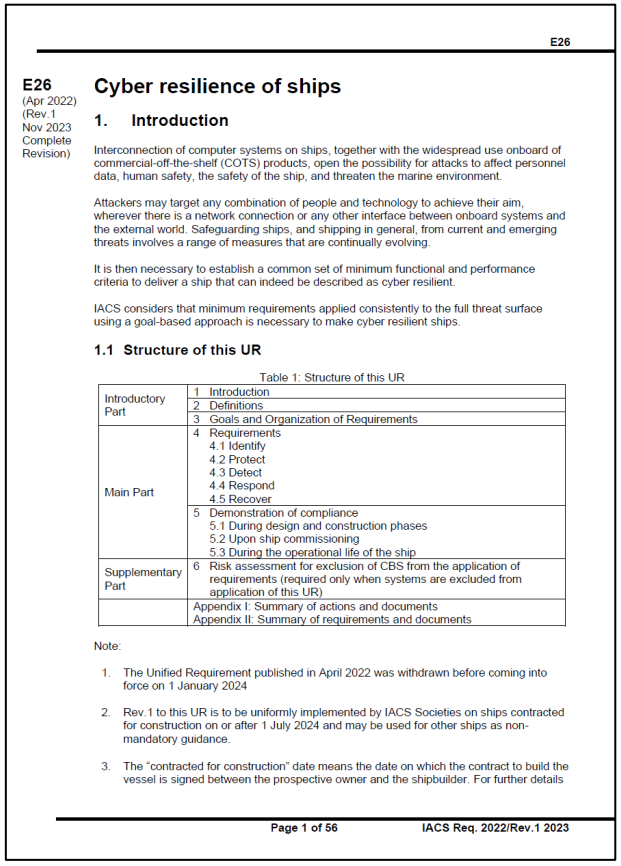
또한, 사이버 공격·위협으로 선박 운항장애 등 해양사고가 발생하거나 발생할 우려가 있는 경우 해운선사는 그 사실을 바로 해양수산부에 통보하도록 하며, 해양수산부는 관련 부서·기관에 이를 전파하고 사고대응, 복구 지원 및 사고원인 조사 등을 실시하도록 명시하였다.

최근 자율운항선박 개발, 정보통신기술 발달로 육상과 선박을 잇는 디지털 통신망·시스템이 급격히 발전하면서 사이버안전의 중요성이 더욱 커지고 있다. 실제로 2017년에는 컨테이너선 항법장치가 사이버 공격을 받아 약 10시간 동안 선박운항 통제권이 상실되는 일이 있었으며, 2019년에는 자동차운반선 내부 시스템이 악성파일(랜섬웨어)에 감염되어 삭제되는 사례가 있었다.

1. 해사 사이버 공격으로부터 선박운항시스템 등을 보호하고, 선박 및 사업장의 효율적인 해사 사이버안전 관리 지원 목적
2. 안전 관리 체제(SMS) 갖춘 선박 및 사업장에 적용
3. 표준 지침서(매뉴얼) 제작·발표 및 영세 선사 대상 사이버안전 진단 · 실태 평가 시범 사업 실시
4. '해사 사이버안전 종합대책' 수립
5. '24년 '해사 사이버안전 관리 강화 방안 연구 용역' 수행 중
   - 해사 사이버안전 관리체계 구축 시범 사업
   - 민관 해사 사이버안전 교육 훈련 시범 사업
   - 해사 사이버 안전법제화 기반 구축

해양수산부 해사 사이버안전 관리 강화 방안

선박 사이버 복원력 (UR E26)



E26

E26
(Apr 2022)
(Rev.1
Nov 2023
Complete
Revision)

Cyber resilience of ships

1. Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment.

Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving.

It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient.

IACS considers that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships.

1.1 Structure of this UR

Table 1: Structure of this UR

Introductory Part	1 Introduction 2 Definitions 3 Goals and Organization of Requirements
Main Part	4 Requirements 4.1 Identify 4.2 Protect 4.3 Detect 4.4 Respond 4.5 Recover
	5 Demonstration of compliance 5.1 During design and construction phases 5.2 Upon ship commissioning 5.3 During the operational life of the ship
Supplementary Part	6 Risk assessment for exclusion of CBS from the application of requirements (required only when systems are excluded from application of this UR)
	Appendix I: Summary of actions and documents Appendix II: Summary of requirements and documents

Note:

1. The Unified Requirement published in April 2022 was withdrawn before coming into force on 1 January 2024
2. Rev.1 to this UR is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 July 2024 and may be used for other ships as non-mandatory guidance.
3. The "contracted for construction" date means the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. For further details

Page 1 of 56 IACS Req. 2022/Rev.1 2023

01 ◆ 발효시점 : 2024년 7월

이 UR은 2024년 7월 1일 이후에 건조 계약된 선박에 대해 IACS 선급협회에 의해 일관되게 적용되어야 하며 그 외 선박들에 대해서는 비강제 지침으로 사용될 수 있다. 이 UR의 비강제 시험 적용을 위한 충분한 시간을 허용하기 위해 적용 일자는 2024년 1월 1일로 선택되었다.

02 ◆ 선박 사이버 복원력 (Cyber Resilience)

이 UR의 목표는 이해 관계자에게 사이버 복원력을 가진 선박으로 이어지는 기술적 수단을 제공할 목적으로 선박 사이버 복원력(Cyber Resilience)에 대한 최소 세트의 요구사항을 제공하는 것이다.

*선박의 안전한 운항을 위해 사용되는 운영기술(OT)의 중단 또는 손상으로 인해 발생하는 사 발생을 줄이고 영향을 완화하는 기능을 의미한다

선박 사이버 복원력 (UR E26)

03 ◆ 적용선박(Mandatory)

(1) 국제항해에 종사하는 여객선
(2) 국제항해에 종사하는 500GT 이상의 화물선
(3) 국제항해에 종사하는 500GT 이상의 고속선
(4) 500GT 이상의 이동식 해양 시추선
(5) 건설에 종사하는 자체 추진 이동식 해양 구조물(예: 풍력 터빈 설치, 유지 보수 및 수리, 크레인 유닛, 시추부속선(tender), 숙박 시설 등)
(비고) 이 지침은 다음에 대하여 비강제 지침으로 사용할 수 있다. (예, 총톤수 500톤 미만의 화물선 등)

04 ◆ 적용 시스템

(1) 선박 내 운영기술(OT) 시스템

- Propulsion
- Steering
- Anchoring and mooring
- Electrical power generation and distribution
- Fire detection and extinguishing systems
- Bilge and ballast systems, loading computer
- Watertight integrity and flooding detection
- Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)
- Any required safety system whose disruption or functional impairing may pose risks to ship operations (e.g. emergency shutdown system, cargo safety system, pressure vessel safety system, gas detection system, etc.)

(2) 항해 및 통신 시스템

- Navigational systems required by statutory regulations
- Internal and external communication systems required by class rules and statutory regulations

(3) 지침 적용 범위의 CBS와 IP 기반 통신 인터페이스

(비고) 상기 다른 시스템의 예는 다음과 같으며 이에 국한되지 않음

1) 여객 또는 방문객 서비스 및 관리 시스템
2) 여객 대상 네트워크
3) 관리 네트워크
4) 선원 복지 시스템
5) 영구 또는 일시적(예, 유지보수 중) OT 시스템에 연결되는 어떠한 기타 시스템

국내선사 실태조사 결과

점검 체크리스트

■ **일반 현황 조사**

- 보안관리조직, IT장비 및 보안솔루션, 사고 사례 등

■ **해사 사이버보안 요구사항**

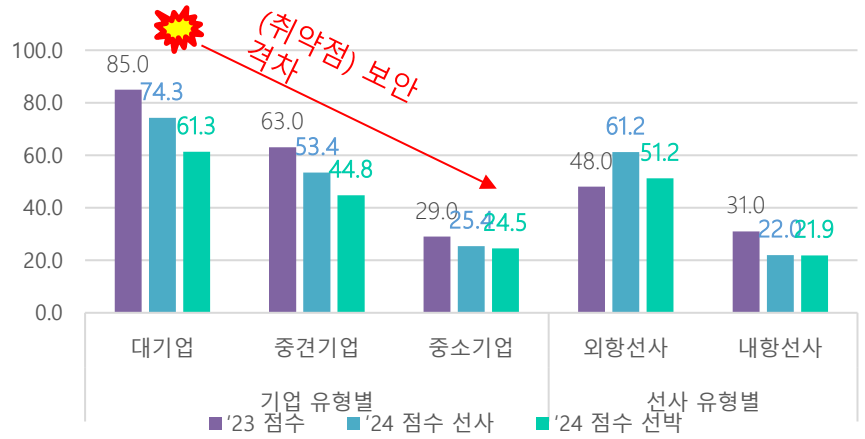
- IMO 요구사항을 충족하는 **KRCS0** 및 **해사 사이버안전 관리 지침(고시)**에 해당하는 항목을 성숙도 관점에서 이행 현황을 평가

■ **국내 정보보호 관련 법률 점검**

- **개인정보 보호법**을 통해 여객 및 선원 개인정보 보호 현황 점검
- **산업기술 보호법을** 통해 국가핵심기술(LNG선 도면 등) 및 중요 정보 관리현황을 평가함

No	업체명	분류	선종	보안 수준		선박 사고 사례
				선사	선박	
1	A 선사	대기업	LNG	42.6	46.9	-
2	B 선사	대기업	Container	69.1	53.1	랜섬웨어 '19년 (4척)
3	C 선사	중견	LNG	75.0	57.8	랜섬웨어 '19년
4	D 선사	중소	내항 여객선	21.2	20.3	(장애발생)
5	E 선사	중소	내항 여객선	22.7	23.4	랜섬웨어 '19년(1척) '20년(1척), '23년(9척)
6	F 선사	중견	BULK	27.9	21.9	(피싱메일)
7	G 선사	대기업	Container	94.1	89.1	(장애발생)
8	H 선사	중견	LNG	57.4	54.7	PC 바이러스 '23년
9	I 선사	중소	오일 케미컬	32.4	29.7	-
10	J 선사	대기업	VLCC	91.2	56.3	-

국내선사 실태조사 결과



구분	'23년 설문조사 결과	'24년 실태조사 결과
점검 기준	NIST 800-52	NIST 800-52 + KRCS0 (IMO요구사항) 및 국내 정보보호 관련 법률
대상	85개 업체 설문조사 (내항/외항 화물 운송, 내항/외항 여객운송, 안전관리대행업)	10개 선사 및 10척의 선박 실태조사

• '23년 설문조사와 '24년 실태조사의 점수 차이
비전문가인 안전품질, 해무팀 등에서 작성하여 객관적인 보안수준측정의 한계

• 기업 유형별 보안 격차
(중견기업) 사이버안전 관리체제는 갖추고 있지만, 보안 유지와 개선에 있어 대기업에 비해 자원과 인력이 부족함

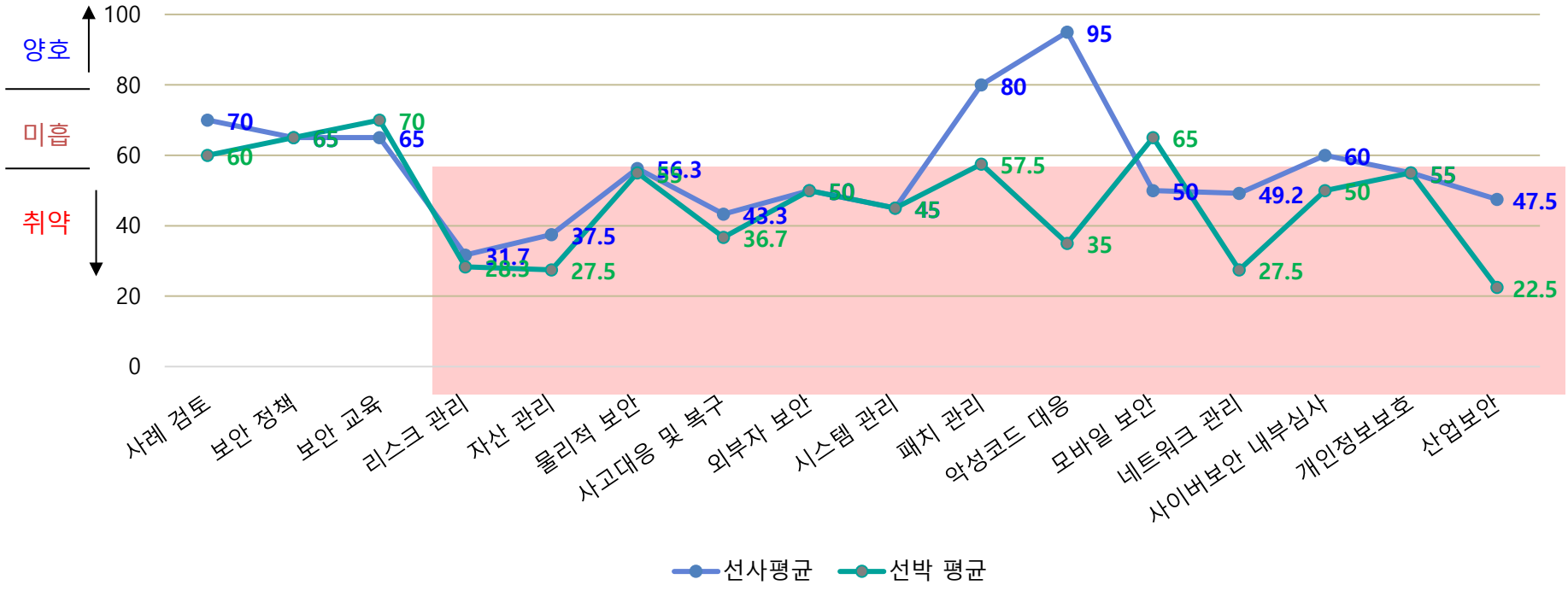
(중소기업) 보안 인프라와 전문 인력의 부족으로 인해 지속적인 사이버 보안 위협에 노출

• 선사 유형별 보안 격차
(내항선사) 국제 규제를 적용 받지 않아, 보안 수준과 관심이 저조하고 사이버사고 인식 부족 및 대응 체계 부재

• 기업 유형별 맞춤형 관리체제 설계 필요
대기업과 중소기업, 외항선사와 내항선사의 보안 수준에 따른 맞춤형 대응 체계 필요

• 인력 및 인프라 투자 확대 필요
중소기업 및 내항선사의 보안 인프라와 전문 인력 부족 문제를 해결하기 위해 정부 차원의 지원과 체계적인 교육 필요

국내선사 실태조사 결과



- 양호 (80~100%) :관리체계가 효과적으로 운영되고 있으며, 주요 취약점이나 위협이 거의 없음
- 미흡 (60~79%) : 일부 보안 제어가 부족하거나 관리체계가 미흡해 사이버 위협에 취약한 상태
- 취약(60% 미만) : 주요 보안 통제가 부재하거나 관리체계가 거의 없으며, 심각한 보안 위험이 존재함

요약

- 선박 통신환경의 급격한 발전으로 인한 사이버 리스크가 높아지고 있음
- 선박 사이버보안 국제규제(IMO 및 주관청 등)는 점점 강화되는 추세
- 미국 USCG는 입항하는 모든 선박에 사이버 리스크 관리가 안전관리체계(ISM)에 통합되어 있지 않은 경우 출항정지(Code 30) 할 수 있음
- 해양수산부는『선박 사이버안전 법』입법을 준비 중
- 국내 선사 사이버보안 실태조사 결과, 미흡한 점이 다수 발견됨
- 따라서, 선박 사이버보안에 대한 인식 개선이 필요하며, 관련 인력 및 인프라 투자 확대가 필요

Thank you for your attention!

Any Questions?

Providing the best service,
Creating a better world