# 船舶サイバーセキュリティ規制の最新動向

## ― IACS UR E26/E27と本会の取り組み ―

技術本部　機関部，認証本部　認証・海技部

## 1. はじめに

近年，船舶のデジタル化が急速に進み，サイバー攻撃のリスクが高まっている。海事業界でのランサムウェアによる被害額の急増や，実際に船舶へのサイバー攻撃が行われたという報告がされている。そのような背景から船舶のサイバーセキュリティが注目され，国際船級協会連合（以下，IACS）はIACS統一規則（以下，UR）E26及びE27を策定し，2024年7月1日建造契約船から適用が開始された。本稿ではUR E26とE27を中心に，船舶のサイバーセキュリティ規制の背景や動向，そして本会の取り組みについて概説する。

### 1.1　船舶を取り巻くサイバーセキュリティ上の脅威

従来，船舶の航海設備，機関制御装置，貨物監視装置などのシステムは物理的な接続や制御に依存しており，サイバー攻撃等の脅威は想定されていなかった。しかし，運航効率化や安全性強化のためにIoT技術が導入され，近年では米国SpaceX社が提供するStarlinkなどの比較的安価かつ大容量な洋上インターネットサービスも開始されたこと，さらには開発が進められている自動運航技術の採用などから，舶用システムがコンピュータやインターネットを介して相互接続されるケースが増加している。これに伴い，舶用システムはサイバー空間に晒される機会が増え，サイバー攻撃のリスクが顕在化している。

米国にある海事分野に特化したサイバーセキュリティ情報共有・分析機関であるMTS-ISAC[*1]の統計によると，2024年6月の海事分野に対するサイバー攻撃のうち，船舶への攻撃は全体の15%を占めている。これは，船舶へのサイバー攻撃が確実に発生しており，その件数が増加傾向にあることを明確に示している。

このような状況から，海事業界ではサイバーセキュリティへの関心が高まっており，船舶に対しても対策が求められている。

具体的なサイバー攻撃手法としては，ランサムウェアによる船舶管理システムの乗っ取り，GPSスプーフィングによる位置情報の偽装，フィッシング詐欺による乗組員の個人情報の窃取などが報告されている。**表1**に主な攻撃事例を示す。

**表1　サイバー攻撃の事例**

| |
|---|
| 2017年6月，海運大手Maersk（マースク）社がNotPetyaと呼ばれるランサムウェアによるサイバー攻撃を受け，世界中の事業拠点が影響を受けた。この攻撃により，同社のコンテナ輸送業務が混乱し，数億ドル規模の損失が発生したとされている。 |
| 2017年6月，黒海において，少なくとも20隻の船舶のGPS受信機が，実際には海上にいるにも関わらず，約32km内陸の位置を示すという異常が発生した。この現象は，GPSスプーフィング[*2]攻撃によるものと強く疑われている。 |
| 2019年5月，米国沿岸警備隊（USCG）が発行したMarine Safety Information Bulletinによると，PSC当局を装ったメールアドレスから船舶へメールを送信し，到着通知に含まれる機密情報を抜き取ろうとする事例が報告されている。 |
| 2023年1月，DNV社の提供する船舶管理用ソフトウェアのサーバーがランサムウェア攻撃を受け，オンライン機能へのアクセスが制限された。 |

*1　海事交通システム情報共有分析センター（Maritime Transportation System Information Sharing and Analysis Center）の略称である。海事分野におけるサイバーセキュリティに関する情報共有や分析を行う組織である。

*2　偽のGPS信号を発信することで，GPS受信機の位置情報を誤認させるサイバー攻撃の一種。船舶の航路を狂わせたり，衝突事故を引き起こしたりする危険性がある。

これまでの報告事例から，船舶のITシステム*3がランサムウェアやマルウェアなどのサイバー攻撃の標的となっていることは明らかである。一方，OTシステム*4（船用システム）へのサイバー攻撃の影響については，具体的な被害状況や攻撃手法などの詳細が公開されるケースが少なく，依然として不明な点が多いのが現状である。その原因としては，サイバーセキュリティ対策が不十分な場合，攻撃を受けたこと自体に気付くのが難しいことが挙げられる。また，攻撃の詳細情報を公表すると，企業の評判低下や取引先からの信頼低下につながる可能性や，更なるサイバー攻撃を誘発するなどのリスクがあることも，情報公開をためらわせる背景となっているようである。

### 1.2　国際的なサイバーセキュリティ対策の動向

船舶のサイバーセキュリティリスクの高まりを受け，国際海事機関（以下，IMO）やIACSは，船舶のサイバーセキュリティ対策の強化に取り組んでいる。

#### 1.2.1　IMOの取り組み

IMOは，船舶のサイバーセキュリティに関する取り組みを段階的に強化している。

・ISPSコード

2004年に採択されたISPSコード（国際船舶・港湾施設保安コード）は，船舶や港湾施設の物理的なセキュリティ対策に重点を置いている。直接的にサイバーセキュリティ対策を求めるものではないが，船舶保安評価（SSA）及び船舶保安計画（SSP）において，コンピュータシステムやネットワークの脆弱性への対処，ならびに電子形式の機密情報の保護に関する手順の確立を求めている。これらは，サイバーセキュリティ対策の基礎となるものである。ISPSコードは，SOLAS条約（海上人命安全条約）の締約国に対して強制力を持つ。

・決議MSC.428(98)

2017年に採択された決議MSC.428(98)は，船舶の安全管理システム（SMS）にサイバーリスク管理を組み込むことを推奨している。これは，サイバーリスクを船舶の運航における他のリスクと同様に評価し，適切な対策を講じることを求めるものである。この決議は推奨事項だが，多くの旗国が強制化している。

・GUIDELINES ON MARITIME CYBER RISK MANAGEMENT（MSC-FAL.1/Circ.3）

決議MSC.428(98)の実施を支援するため，2017年に承認*5されたガイドラインである。船舶の運航者や船主がサイバーリスク管理を実施する際に役立つ，船会社の役割，活動，対策に関する具体的な推奨事項が記載されている。また，IACS，バルチック国際海運協議会（以下，BIMCO），米国国立標準技術研究所（以下，NIST）*6などが発行するサイバーセキュリティに関するガイドラインや規格を参照している。このガイドライン自体は強制力を持たないものの，船舶の運航者や船主が効果的なサイバーリスク管理体制を構築・運用するための参考となる。

#### 1.2.2　IACSの取り組み

IACSは，2016年にサイバーシステムパネルを設置し，各船級協会の専門家が集まり，最新のサイバーセキュリティ技術や脅威に関する情報共有，及び統一規則の策定に向けた議論を行ってきた。

・12のIACS Recommendations（以下，Rec.）

2018年11月までに12のRec.を公表している。これらの勧告は，船舶のサイバーセキュリティ対策に関する具体的な指針を示しており，ソフトウェアの保守手順，機器の手動/機側制御，緊急時対応計画，ネットワーク構造，データの保証，物理的セキュリティ，ネットワークセキュリティ，船舶システムデザイン，インベントリリスト，インテグレーション，遠隔アップデート／アクセス，通信及びインターフェースといった広範な領域をカバーしている。

・Rec. No. 166

UR E26とE27の策定に先立ち，上記の12のRec.を一つに統合する作業を実施し，2020年5月にサイバー

*3　情報技術（Information Technology）システムの略称である。データの収集，処理，保管，伝達などを行うシステムである。船舶では，事務作業用のPCなどが該当する。
*4　運用技術（Operational Technology）システムの略称である。物理的なプロセスや設備の監視，制御を行うシステムである。船舶では，船舶の航海設備，機関制御装置，貨物監視装置などのシステムも該当する。
*5　定期的に更新が行われており，2022年にはMSC-FAL.1/Circ.3/Rev.2が承認されている。
*6　技術，測定，標準に関する研究開発を行う米国政府機関である。サイバーセキュリティ分野でも様々なガイドラインやフレームワークを策定している。

レジリエンスに関する推奨事項としてRec. No. 166を発行した。これは，新造船の建造と運航において推奨されるサイバーセキュリティ対策をまとめたものである。船舶の設計・建造・運航の各段階で考慮すべき事項を包括的に示しており，具体的には，リスク評価に基づいた対策，ネットワークの分離，アクセス制御，システムの更新，乗組員の教育などが含まれる。

・UR E26とE27

IACSは，それまでの取り組みで得られた成果を基に，2022年4月，サイバーセキュリティに関する要件を定めたUR E26とE27の2つのURを新たに策定した。これらは，サイバー攻撃を受けるという前提に立ち，サイバー攻撃等によるサイバーインシデントの発生を低減し，影響を軽減し，障害等が発生した場合でも早期に復旧する機能（以下，サイバーレジリエンス）に関する要件である。主に，UR E26では船舶全体のサイバーレジリエンスの枠組みを，UR E27では船舶に搭載されるシステム及び機器のセキュリティ要件を規定している。これらのURの目的は，サイバーレジリエンスを最低限確保した船舶を実現することにある。

当初，UR E26及びE27については2024年1月1日から施行される予定であったが，適用対象船舶の限定，検査要件の明確化，そして業界からのフィードバックを踏まえ，IACSはUR E27を2023年9月に，UR E26を同年11月にそれぞれ改訂した。そして，これらの改訂版は，2024年7月1日以降に建造契約を締結する船舶から適用が開始されている。*7

## 2. UR E26とE27の要件の目的と概要

本章では，UR E26とE27の要件の目的と概要を解説する。なお，要件の詳細については，3章で紹介するガイドラインで解説しているので，そちらを参照してほしい。

### 2.1 UR E26とE27の関係

UR E26は船舶全体のサイバーレジリエンス確保のための包括的な枠組みを規定し，UR E27はUR E26の適用範囲内の個々のシステム・機器に対する具体的な技術的要求事項を規定している。また，UR E26は関係者の連携と責任分担を明確化し，UR E27は機器供給者の責任においてコンピュータシステムのセキュリティ確保を要求している（図1）。

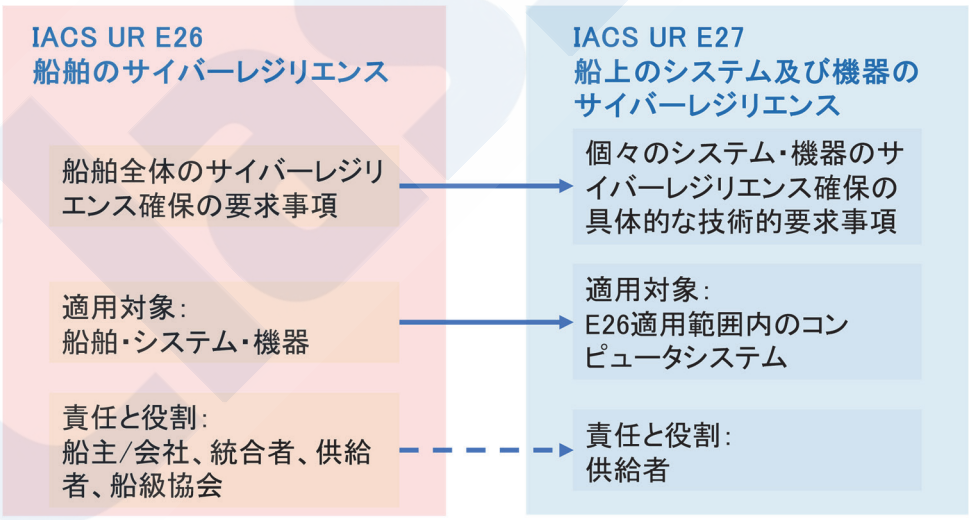


図1 UR E26とE27の関係

### 2.2 UR E26の要件の目的と概要

UR E26は船舶全体を対象とする規則であり，主に造船所（統合者）と船主が関わる要件を規定している。具体的には，船舶の設計，建造，試運転，運航といった各段階を通じて，運用技術（OT）システムや情報技術（IT）システムを船舶のネットワークに安全に統合することを目的として，「識別」「防御」「検知」「対応」「復旧」といった要件を規定している。

*7 当初のバージョンは適用開始前に取り下げられた。

### 2.2.1　UR E26の目的とNISTサイバーセキュリティフレームワーク

UR E26の要件は，Rec. No. 166，各船級協会のガイドライン，BIMCOガイドライン，NIST SP 800-53などを参考に，NISTサイバーセキュリティフレームワークの5つの機能要素（**図2**）で整理・規定している。そして，船舶の特性に合わせて，それぞれの目的を以下のように整理している。

- 識別（Identify）…船舶のシステムやそこに携わる人，データ，機器などを把握し，サイバーセキュリティ上のリスクを洗い出し，組織として理解を深める。
- 防御（Protect）…サイバーインシデントから船舶を守るための対策を講じ，万が一攻撃を受けたとしても，船の運航を継続できるようにする。
- 検知（Detect）…サイバーインシデントの兆候をいち早く捉え，特定するための仕組みを構築する。
- 対応（Respond）…サイバーインシデントを検知した場合，被害を最小限に抑えるための対応策を実施する。
- 復旧（Recover）…サイバーインシデントによって船舶の機能が損なわれた場合，速やかに復旧するための手段を確保し，通常運航に戻す。


**図2　NISTサイバーセキュリティフレームワークの5つの機能要素**

### 2.2.2　UR E26の適用対象船舶

以下の船舶等に適用される。

- 国際航海に従事する旅客船（旅客船に該当する高速船を含む）
- 国際航海に従事する総トン数500トン以上の貨物船
- 国際航海に従事する総トン数500トン以上の高速船
- 総トン数500トン以上の海底資源掘削船
- 建設に従事する自航式海洋構造物

内航船や総トン数500トン未満の貨物船への適用は非強制である。

### 2.2.3　UR E26の適用対象システム

サイバーインシデントの影響により，人の安全，船舶の安全，または環境に危険を及ぼしうる，以下の機能を持つ船上のOTシステムに適用される。

(a)　推進
(b)　操舵
(c)　投錨及び係留
(d)　発電及び分電
(e)　火災探知及び消火システム
(f)　ビルジ及びバラストシステム，積付計算機
(g)　水密性及び浸水検知
(h)　照明（例えば，非常灯，低位置照明，航海灯等）
(i)　要求される安全システムであって，当該システムの途絶又は機能障害が船舶の運用にリスクをもたらしうるもの（例えば，緊急停止システム，荷役安全システム，圧力容器の安全システム，ガス検知システム等）
(j)　条約により要求される航海設備
(k)　船級規則又は条約により要求される船内及び船外通信システム

また，UR E26では，これらのOTシステムと接続するすべてのIPベースの通信インターフェースも適用範囲に含まれると規定しており，上記OTシステム以外のシステムや機器についても適用対象となる場合がある。

### 2.2.4 UR E26のリスク評価と適用除外

UR E26では，統合者が，システムが4つの基準を満たし，かつ3つの追加基準を考慮した上で，当該システムをUR E26の要求事項の適用から除外することが適切であると船級協会に説明し，船級協会がそれを承認した場合，そのシステムをUR E26の適用対象から除外できると規定している。

## 2.3 UR E27の要件の概要と目的

UR E27はシステム及び機器を対象とした規則であり，主に舶用機器メーカー（機器供給者）に関わる要件を規定している。具体的には，機器供給者がサイバーレジリエンスの高い機器を開発・製造し，船舶に搭載できるように，システム及び機器のサイバーレジリエンスの要件，船上のユーザーとコンピュータシステムとのインターフェース，そして新規製品の製品開発要件などを規定している。

### 2.3.1 UR E27の適用対象

UR E27では，UR E26に規定される適用対象船舶において，UR E26に規定されるコンピュータシステムに適用されることが規定されている。

### 2.3.2 UR E27のセキュリティ機能の要件

UR E27では，システムに実装すべきセキュリティ機能に関する要件を具体的に規定している。それらの要件は，産業用オートメーション及び制御システムのセキュリティに関する国際規格であるIEC 62443-3-3をベースとしており，その一部が採用されている。具体的には，30の「要求されるセキュリティ機能」と，信頼できないネットワークと接続されたコンピュータシステムに要求される11の「追加で要求されるセキュリティ機能」が規定されている。これらのセキュリティ機能は，コンピュータシステムが備えるべき具体的な対策技術であり，例えば，「認証」「アクセス制御」「暗号化」「マルウェア対策」などが挙げられる。これらの要件を満たすことで，サイバー攻撃によるリスクを低減し，システムの安全性を確保することができる。

### 2.3.3 UR E27のセキュア開発ライフサイクル（SDLC）要件

セキュアな製品の開発及び保守を目的としたライフサイクルに関する要件を規定し，システムや機器の開発において，セキュリティを考慮した開発プロセスを導入することを求めている。具体的には，「秘密鍵の管理」「セキュリティアップデートの文書」「依存コンポーネント又はオペレーティングシステムのセキュリティアップデート文書」「セキュリティアップデートの配信」「製品の多層防御」「環境において期待される多層防御策」「セキュリティ強化指針」といった7の要件が規定されている。これにより，開発段階からセキュリティ上の脆弱性を排除し，より安全なシステムを構築することができる。

# 3. UR E26とE27に関する本会の取り組みとサポート

サイバーセキュリティ対策が新造船の強制要件として取り入れられることは，UR E26とE27の要件が初めてであり，影響も大きいことから，本会は迅速な規則化や情報発信に努めてきた。要件への対応が必要となる舶用機器メーカー，造船所，船主向けにURの要件を解説するNK独自のガイドライン発行，要件への適合のための具体例を挙げたインタラクティブなワークショップの開催，解説動画などの情報提供をしている。

## 3.1 本会規則へのUR E26とE27の取り入れ

本会では，UR E26及びE27の発行を受けて，これらの要件を本会規則に取り入れた。2つのURを鋼船規則X編並びにB編及び船用材料・機器等の承認及び認定要領に取り入れるために，有識者からなる専門委員会（2023年12月），技術委員会（2024年1月）の審議を経て，2024年6月27日に改正版を発行した。

**図3**は，2つのURの要件を主に規定している鋼船規則X編の構成である。

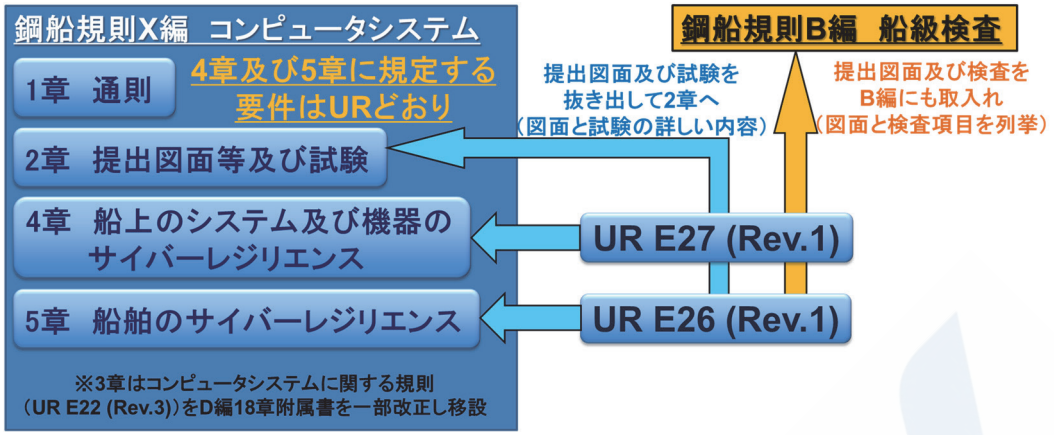


図3 UR E26とE27の本会規則への取り入れ（鋼船規則X編の構成）

船用材料・機器等の承認及び認定要領では，第7編10章にサイバーレジリエンスに関する対策が講じられる機器等の使用承認*8のための規定を新設した。これにより，舶用機器メーカーが，船舶への搭載準備をする前に，サイバーセキュリティ要件を満たした機器等が規定に適合していることを証明する使用承認証書を事前に取得できるようにしている。

### 3.2 UR E26とE27の要件を解説するガイドライン

まずは，サイバーセキュリティ要件を満たした機器等がマーケットに出揃うことが必要と考え，機器等の要件を規定するUR E27を解説するNK独自のガイドライン「船上のシステム及び機器のサイバーレジリエンスに関するガイドライン」を2023年11月に発行した。

さらに，2024年7月にはUR E26の要件を解説するNK独自のガイドライン「船舶のサイバーレジリエンスに関するガイドライン」を発行した。**図4**は各ガイドラインとその構成である。


図4 UR E26とE27の要件を解説するガイドラインとその構成

特に2つのNK独自のガイドラインについては，URには記載のない例示を多くすることで解説本としての「分かりやすさ」を目指した。例えば，サイバーセキュリティの要件が適用になる機器は機関制御装置，操舵システム制御装置，固定式炭酸ガス消火装置，航海用レーダー，などと具体的に例示している。**図5**に例示の一部を示す。

*8 船舶への搭載準備をする前に，その使用に関してあらかじめ本会の承認を得ることが規則等で定められている船用機器等について，あらかじめ代表的な個品に対して承認要領に規定された審査，試験及び検査を行い，当該機器が当該規定に適合していることを承認する。

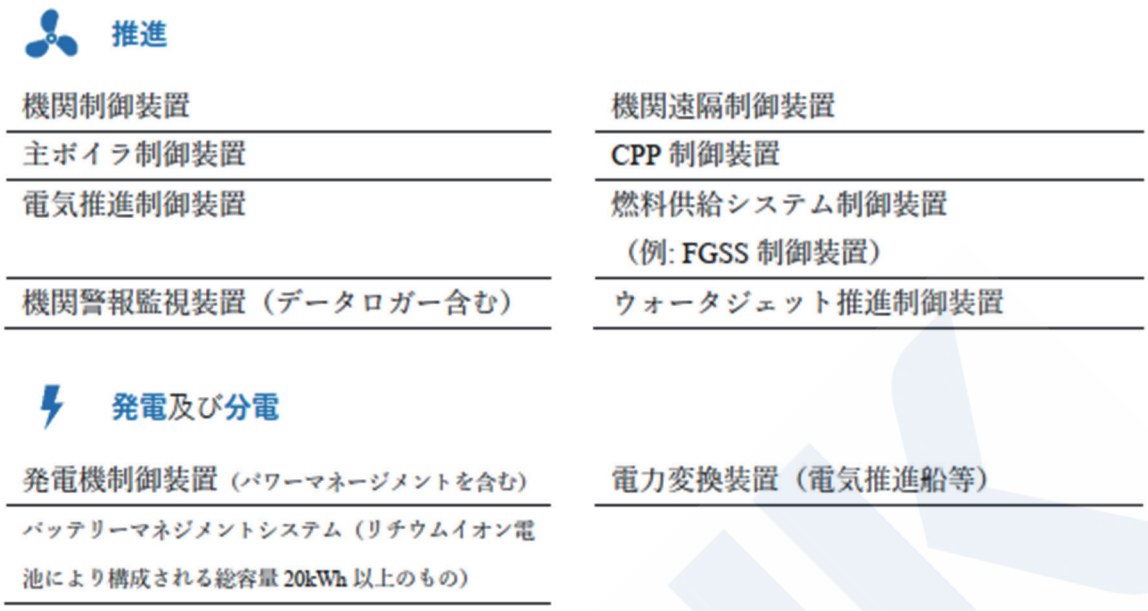


図5　ガイドラインにおける適用対象システムの例示

### 3.3　ポータルページ

本会ホームページでは，解説動画やFAQ（適宜アップデート）を提供している。これらはすべてホームページ上のUR E26/E27に関する情報や資料を集約したポータルページで閲覧することが可能となっている。（https://www.classnk.or.jp/hp/ja/activities/cybersecurity/ur-e26e27.html）

ポータルページでは以下の情報や資料を提供しており，随時更新中である。

・関連規則
・使用承認申請書
・ガイドライン
・FAQ
・解説動画

### 3.4　ClassNKアカデミー

より専門的に理解を深めたいというご希望のある方々を対象に，ClassNKアカデミーに船用機器の開発者及び設計者を対象とした船上のシステム及び機器のサイバーレジリエンスのコースも新設した。本コースでは，UR E27のベースになっている産業機器のサイバーセキュリティに関する国際規格IEC62443の認証業務に従事されている，技術研究組合制御システムセキュリティセンター（CSSC）より講師を招き，同IEC規格の基本的な考え方から，UR E27で要求されているセキュリティ機能及びセキュア製品開発ライフサイクルについて解説いただいている。

## 4. まとめと今後の展望

本稿では，船舶のサイバーセキュリティ規制UR E26/E27と本会の取り組みを紹介した。船舶を取り巻くサイバーセキュリティ環境は日々変化しており，特に自動運航船のような新技術導入は更なる対策を必要とすることが予想される。

今後の船舶運航はデジタル化・自律化が加速し，サイバー空間の活用が進むだろう。URやIMOガイドラインへの対応に加え，自動化・自律化への対応，脅威情報の収集と共有，セキュリティ人材育成，新技術活用など多角的なセキュリティ強化が必須である。

本会は，安全かつ持続可能な海運の実現を使命とし，船舶のサイバーレジリエンス向上もその重要な要素として捉え，関係者と連携して取り組みを進める所存である。

## 参考文献


1) 中山 公平．船舶におけるサイバーセキュリティ対策の構築に向けた現況．日本マリンエンジニアリング学会誌．2020;55(5):553-556.
2) The Maritime Executive. Mass GPS Spoofing Attack in Black Sea?, Jul 11, 2017, https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.
3) "Maersk Line: Surviving from a Cyber Attack." Safety4Sea, 8 July 2017, https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/.
4) National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, https://www.nist.gov/cyberframework.
5) Marine Safety Information Bulletin (No.04-19) (May 24, 2019) USCG
6) DNV AS. Cyber-attack on ShipManager servers – update. Published: 23 January 2023. Retrieved from https://www.dnv.com/news/cyber-attack-on-shipmanager-servers-update-237931/ .
7) IMO. (2022). Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2).
8) IACS. IACS Recommendations, No. 166 (Apr. 2020) "Recommendation on Cyber Resilience"
9) IACS. IACS Unified Requirements, E26 (Rev.1) (November 2023) Cyber resilience of ships.
10) IACS. IACS Unified Requirements, E27 (Rev.1) (September 2023) Cyber resilience of on-board systems and equipment.
11) IACS. IACS adopts new requirements on cyber safety, https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/
12) IACS. IACS UR E26 and E27 Press Release, https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release
13) 船舶におけるサイバーセキュリティデザインガイドライン（2019年2月）日本海事協会
14) 船舶におけるサイバーセキュリティマネジメントシステム（2019年3月）日本海事協会
15) ソフトウェアセキュリティガイドライン（2019年5月）日本海事協会
16) 船舶におけるサイバーセキュリティデザインガイドライン（第2版）（2020年7月）日本海事協会
17) 船上のシステム及び機器のサイバーレジリエンスに関するガイドライン（第1.0版）（2023年11月）日本海事協会
18) 船舶のサイバーレジリエンスに関するガイドライン（第1.0版）（2024年7月）日本海事協会