船舶のサイバーセキュリティ対策のこれから

株式会社ＭＴＩ　〇柴田　隼吾

1.　はじめに

近年，海運業界においても，デジタル化の波が押し寄せており，船舶機器のコンピューター化や船内ネットワークの高度化,複雑化が進んでいる.また，船陸間の衛星通信に目を向けても，高速なVSAT(Very Small Aperture Terminal)通信サービスの普及が急速に広がっており，さらには，StarlinkやOneWebといった，低軌道衛星(LEO satellite)を利用した，より高速で低価格な船陸間衛星通信サービスも船舶で利用され始めている.

こういった船舶システムの高度化や衛星通信の普及により，運航における環境負荷の低減や安全航行がさらに深度化する一方で，悪意ある第三者による船舶システムへの不正アクセスや操舵の乗っ取りなど，運航における安全侵害や経済的損害などのサイバーセキュリティ上のリスクも懸念されている.

本稿では，これらの状況を踏まえ，船舶のサイバーセキュリティ対策の現状とこれからについて紹介する．船舶のサイバーセキュリティ対策は船主，船舶運航者だけでなく,造船所や舶用機器サプライヤ,船級なども連携して海事業界全体として取り組むべき課題である.

2. 船舶におけるサイバーセキュリティとは

2.1 海事業界における現状

前述のように，船舶においても衛星通信サービスの普及により，インターネットへの常時接続が広がり，船舶の運航データを陸上でモニタリングする[1)]だけでなく，陸上から船上への遠隔接続による船上機器のメンテナンスや更新など，船陸間のデータ共有が急増している．また，舶用機器のコンピュータ一化や，船陸通信の接続に伴い，船舶の内外からのウイルス感染，不正アクセスといったサイバー攻撃に晒されるリスクが高まっている．[2)]

海事業界でこれまでに報告されているサイバーインシデントの具体的な事例としては，図１に示す通り，2017年ごろから陸上の業務システムやインフラなどのIT(Information Technology)機器を対象としたサイバーインシデントが数多く報告されており，例えば，長期のシステム停止により，約330億円(2017年当時)もの被害を受けた事例もある.

船舶そのものを対象としたOT(Operation Technology)機器のインシデント報告件数はまだ少ないが，船舶位置の異常や，操船の乗っ取り事例などが実際に報告されている．船舶での被害件数が少ないのは，船上で機器の故障やトラブルが発生した際に，その原因が物理的な故障なのか，サイバーインシデントなのかを切り分ける手段が，現状の船舶ではほとんど備わっていないという事も一つの原因と考えられる.

■IT機器（主な標的：陸上システム）

事例発生年	被害	原因	被害事例
2017	システム長期停止	ランサムウェア攻撃	Maersk
2018	システム停止	ランサムウェア攻撃	COSCO
2020	データセンター被害	マルウェア感染	MSC
2020	一部システム被害	ランサムウェア攻撃	CMA-CGM

Maersk単体被害総額 約330億円

■OT機器（主な標的：船舶）

事例発生年	被害	原因	被害事例
2017年頃から急増	船舶位置異常	GNSS成りすまし・妨害 Global Navigation Satellite Systems 全地球航法衛星システム。GPS(米国)、準天頂衛星(日本)、GLONASS(ロシア)、Galileo(EU)等の総称	バルト海 黒海 地中海東部中央部 スエズ運河 紅海　付近等

図１　海事業界におけるサイバーインシデントの例

2.2 船舶運航におけるサイバーセキュリティ

サイバーセキュリティで守るべきものとしては，機密性(Confidentiality)，完全性(Integrity)，可用性(Availability)の３大要素が広く知られてい

る．これに分類して，船舶サイバーセキュリティ対策について整理すると，図 2 に示す通り，船上の業務用 PC などの IT 機器においては，情報漏洩防止や情報改竄の防止など，機密性に重きをおく対策が重要であると考えられる．一方で，航海機器やエンジン制御機器などの OT 機器においては，制御の継続稼働や機器の正常動作の担保など，可用性，つまりは「船舶を止めない事」に重きをおいた対策が必要である．

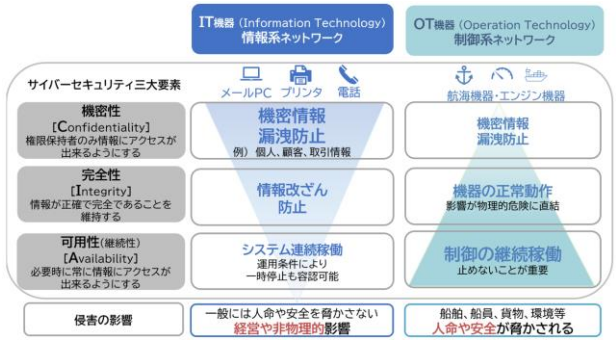

図 2　IT 機器と OT 機器のサイバーセキュリティ対応

船舶に対するサイバー攻撃の手段としては，いくつかの手段と経路が想定されるが，その一つに，図 3 に示す通り船内の IT 機器が接続されている情報系ネットワークに外部からの通信経由，もしくは USB メモリ等を利用して船内部から直接 IT ネットワークに侵入することが考えられる．その後，IT 機器を踏み台にして，IT と OT をブリッジする機器を経由して，OT 機器の接続される舶用機器ネットワークに侵入してくることが考えられる．

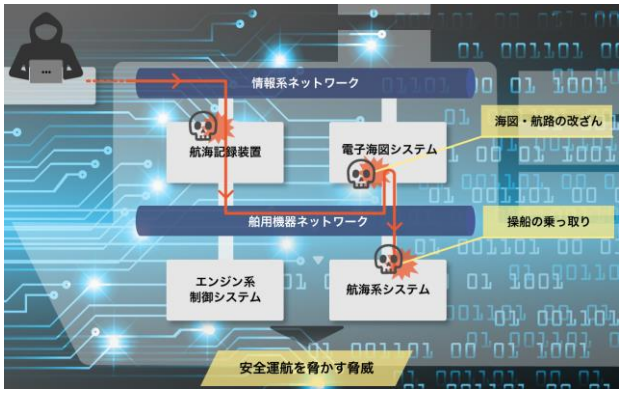

図 3　船舶へのサイバー攻撃のイメージ

3. 業界内での議論と対応

3.1 IMO や船級協会の対応

船舶サイバーセキュリティ対策についての国際的な議論は，2014 年 6 月に開催された，国際海事機関（IMO）第 39 回簡易化委員会（FAL39）から本格化し，2016 年 5 月の IMO 第 96 回海上安全委員会（MSC96）において，船舶運航におけるサイバーリスク管理についての暫定ガイドラインが承認された．その後，2017 年 6 月の MSC 98 において，このガイドラインは MSC 及び FAL の合同回章（MSC-FAL.1/Circ.3 : Guidelines on maritime cyber risk management）[3] として承認され，さらに，海事サイバーリスク管理に関する MSC 決議（MSC.428(98)：Maritime cyber risk management in safety management systems）[4] も採択された．これにより，2021 年 1 月 1 日以降，船主及び運航者は，海上人命安全条約（SOLAS 条約）における国際安全管理コード（ISM Code）に基づき，安全管理システム（SMS: Safety Management System）を通じて，ベースラインのサイバーリスク管理を対策することが強く推奨され，現在，船舶運航者はこれに基づき対策を実施している．

各船級協会においても，2019 年頃から様々サイバーセキュリティ対策の推奨ガイドラインを発行し，ガイドラインに適合した船舶や船舶運航者に対しての任意の船級符号（Notation）の認証などを始めた．さらに国際船級協会連合（IACS）では，2020 年 5 月に Recommendation on Cyber Resilience (REC.No.166) [5] を発行し，新造船の建造と運航において推奨するサイバーセキュリティ対策をまとめた．

そして，IACS は 2022 年 4 月に 2 つの新しい統一規則（UR: Unified Requirement）である，E26: Cyber resilience of ships[6] と，E27:Cyber resilience of on-board systems and equipment[7] を発行した．これらの統一規則は，船舶の OT 機器を対象に，サイバーインシデントに対する耐性の強い船舶の建造と運航に関する規則であり，2024 年 1 月 1 日以降に建造契約する船舶から対象となる．

このように IMO や船級協会での議論や対応は，図

4 に示す通り，ガイドラインなどの任意対応から始まり，徐々に業界内での認識や議論も深まったことで，推奨事項，そして統一規則化と，徐々にその対応と要求レベルも向上してきている．

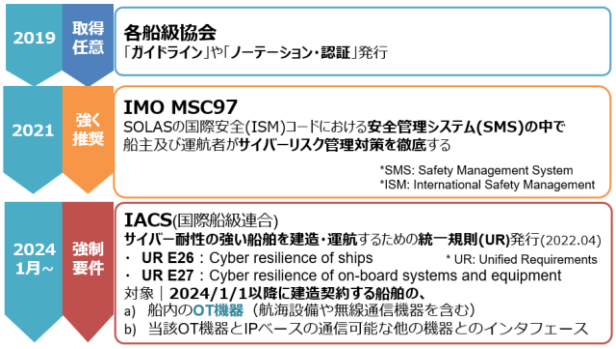

図 4　業界内での議論と対応の流れ

3.2 IACS の統一規則 UR E26, E27

IACS の新しい統一規則である UR E26 と E27 において，その適用対象は，航海設備や無線通信設備も含む船上 OT 機器と，これら OT 機器と IP ベース通信を行う他のシステムとのインターフェース部分までが含まれる．

図 5 に整理した通り，E26 では，船舶全体のサイバーレジリエンス，つまりサイバーインシデントに対する耐性や回復力の高い船舶を実現する事をゴールと定め，そのために設計から建造，運航までの各工程で実施すべき統一的な最低限の要件とその検証方法が記載されている．

それらの要件は，アメリカ国立標準技術研究所(NIST)が発行しているサイバーセキュリティのフレームワークである Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 [8] で定義される 5 つの対応カテゴリ，「特定(Identify)・検知(Detect)・防御(Protect)・対応(Respond)・復旧(Recover)」に分類し，それぞれの実施要件が整理し記載されている．

また，各要件に対する機能評価と検証のための試験法案については今後の改定において詳細が追加される予定である．

一方の UR E27 は，サイバーレジリエントな船上システム及び機器を提供するために，舶用機器ベンダにおける製品の設計や開発に関する要件，および船上機器やシステムの安全性や整合性を担保するための統一的な最低限の要件や，承認のため船級協会に提出が必要なドキュメント類について記載されている．

その要件の主な内容は，工場などの産業用制御システムのサイバーセキュリティ対策規格である IEC62443：Security for industrial automation and control systems の IEC62443-3-3 や IEC62443-4-1 の各要件項目から，船舶に適用可能なものを抜粋および一部修正して記載されているため，これらの IEC 規格も参照して対応実施することが有効である．

2 つの統一規則は 2024 年 1 月以降に建造契約する船舶が対象であるため，あと 1 年程で，舶用機器サプライヤ，造船所，船主，船舶運航者はそれぞれに必要とされる対応を検討し準備していく必要があるが，それぞれが単独で検討するのではなく，各プレーヤが連携し，さらには船級やサイバーセキュリティ専門家とも十分に連携していく必要がある．

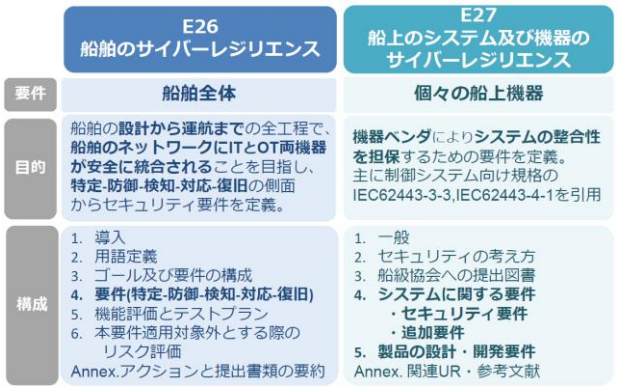

図 5　IACS 統一規則 UR E26 と E27

4. 今後必要とされる対策

4.1 安全対策とサイバーリスク管理

前述の通り，船舶サイバーリスク管理では，船上 OT 機器を守ることが重要であり，それにより安全運航を継続するために必要な各機能を正常に継続稼働させることにある．

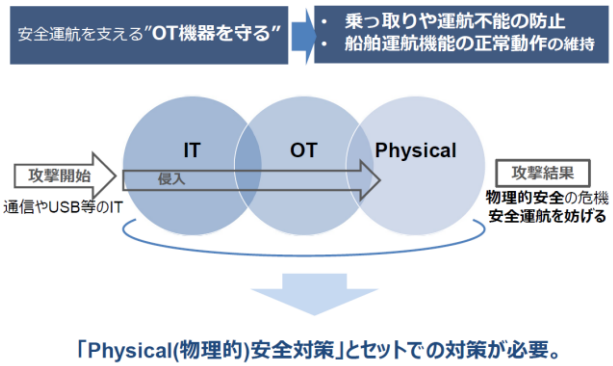

図 6　船舶運航におけるサイバーリスク管理

図 6 に示す通り，船舶のサイバーインシデントの原因となる攻撃は，不正な通信や USB メモリなど目に見えにくい「Cyber」なポイントから始まり，それが急速に広がり，さらに船上 OT 機器の正常動作に影響を及ぼし，最終的に安全運航を妨げる目に見えやすい「Physical」へと影響していく．つまり，船舶運航におけるサイバーリスク管理とは，Cyber と Physical を一体にして考える必要があり，IT 担当者やサイバーセキュリティの専門家だけに任せて実施するものではなく，これまで長年にわたり積み重ねてきた物理的な安全運航の対策や取り組み，さらには既存の安全管理組織とも十分に連携して実施する必要がある．

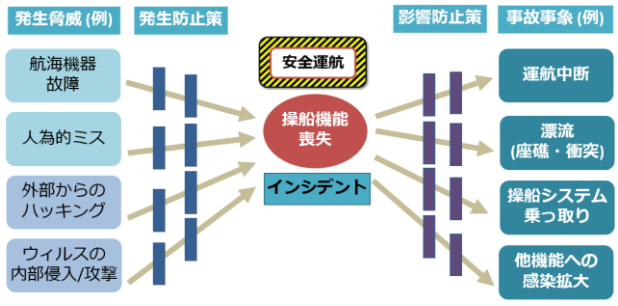

図 7　Bow-Tie リスクアセスメント手法による整理

Cyber と Physical が連携した安全対策について，Bow-Tie(蝶ネクタイ)型のリスクアセスメント手法を用いて考察する(図 7)．まず Bow-Tie 図の中央に安全運航を阻害するインシデントを置き，その左側にインシデント発生原因(=発生脅威)，右側には，インシデントが発生してしまった後にその影響が広がることによる事故事象を定義する．

例えば「操船機能の喪失」というインシデントを中央に設定すると，既存の物理的な安全対策では，発生脅威(図の左側)には，「機器の物理的故障」や「人為的ミス」などが挙げられる．それら脅威がインシデント(図の中央)に繋がらないように，バリアとして「センサーデータによる故障予知診断」や，「BRM: Bridge Resource Management 訓練」などの多重の発生防止策がある．さらに，事故事象(図の右側)には，「運航中断」や「座礁・衝突」などが挙げられ，ここでも，中央のインシデント発生から右側の事故事象に影響が広がらないように，「早期発見」や「復旧」のための多重のバリアを設けている．

この物理的な安全対策の Bow-Tie 図に，さらにサイバーセキュリティを追加すると，脅威としては「ハッキング」や「ウイルスなどの侵入／攻撃」が挙げられ，さらにインシデント発生後の事故事象としては，「操船の乗っ取り」や「他機器・他船・陸上システムへの感染拡大」などが追加される．ここにも，発生防止策と影響拡大防止策の多重のバリアをそれぞれ設ける必要がある．

サイバーセキュリティ対策のバリアを設置する上でポイントは 2 つある．サイバー脅威は物理的な脅威に比べると，①脅威である攻撃の初期症状が発見しづらい．また，②初期対応が遅れると影響の拡大が速く，影響範囲も広くなると言った特徴があり，それらを考慮してバリアを設置していく必要がある．

4.2 サイバーリスク管理の向上

船舶運航者における船舶サイバーリスク管理は IMO で推奨されている通り，安全管理システム (SMS) を通じて現在すでに対策実施しているが，今後，その対象範囲を拡大させ，さらに対策内容の深度化をしていく必要があると考える．

具体的には，これまでは，既存船の船上 IT 機器システムの対策が中心であったが，これを前述の IACS のサイバーレジリエンスに関する統一規則で求められる OT 機器システムにもその対象範囲を広げていく必要がある．

対策内容では，NIST の Framework for Improving Critical Infrastructure Cybersecurity で定義される「特定」「防御」「検知」「対応」「復旧」の 5 つのカテゴリにおいて，現時点でも最低限の対策は実施されているが，それぞれの内容を IACS の統一規則で求められるサイバーレジエンスを念頭にした内容に深度化させる必要がある．

特に深度化が必要なのは，「検知」の部分である．つまり，船上のサイバー脅威を早期かつ的確に検知する仕組みの実現である．これは船内 IT 機器ネットワークのみならず，OT 機器やネットワークにおいても，検知の仕組みが必要である．さらに，その検知した脅威やインシデントを陸上で統合的に監視し，船舶運航者が，船やサイバー専門家，既存の安全対策組織，機器サプライヤとも密に連携して，インシデントや事故を未然に防ぐために早期に「対応」・「復旧」する組織横断型の連携体制の構築や人材育成・教育が急務である．（図 8）

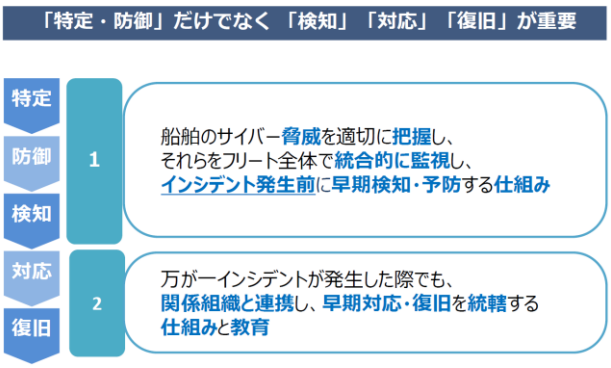

図 8　おけるサイバーリスク管理の拡充ポイント

4.3 サイバーレジリエンスの向上

IACS の新しい統一規則によるサイバーレジリエンス対応により，航海機器や機関制御装置など船舶の OT 機器・システムの機器ベンダにおいても，サイバーセキュリティ対策機能の追加開発や，機器システムの脆弱性の検査や承認などの対応が必要となってくる．さらに，複数の OT・IT 機器を統合した船舶全体のシステムとしても，サイバー脆弱性の検査や対策が必要である．これらの実施は船舶の設計・建造時のみならず，就航後にもシステム構成を変更した際などに定期的に実施が必要となってくる．

サイバー脆弱性の調査において有効な手法としては，ペネトレーションテスト（Penetration Test）という脆弱性診断手法がある．

弊社が 2020 年に海事業界の各関係者と合同で実施した船舶システムへのペネトレーションテスト検証の結果，船舶建造におけるテスト実施のタイミング，実施主体者，実施範囲については，機器サプライヤだけでなく，造船所，船主，運航者での建造計画段階からのしっかりとした議論と，さらには効率的なテスト実施体制の構築が必要であることが分かった．この検証結果は「船上機器システムにおけるサイバーリスク対策検討のためのペネトレーションテスト成果報告書」[9] として公開されているのでぜひご参考いただきたい．

また，海外での参考になる先行事例としては，英 Plymouth 大学にある Cyber-Ship lab と呼ばれるラボ施設がある．このラボには，実際の航海計器や機関系システム，カーゴ管理システムなど，複数メーカの舶用機器が備わっており，それらを組み合わせた船舶システムの模擬環境が陸上に構築されている．そこでは，船舶サイバーセキュリティに関する教育・トレーニングの実施のみならず，舶用機器サプライヤが新たな機器を持ち込んでのペネトレーションテストなども実施している．

今後，日本においてもサイバーレジリエンスな船舶を建造し運航していくためには，こういった事例も参考にして，OT 機器のサイバーレジリエンス機能の検査や，船級による承認の仕組みなども構築していく必要がある．

5. まとめ

本稿では，船舶サイバーセキュリティ対策の現状とこれから必要とされる対応について，特に，2024 年 1 月以降に対応が必要となる IACS のサイバーレジリエンスに関する統一規則を念頭におき，船舶運航者や機器ベンダ，造船所，船級，サイバー専門家などが連携して取り組むべき課題について述べた．

船舶の安全運航のためには，これまでの物理的な安全対策とサイバー対策とを十分に連携させた対策が必要となり，船舶の IT および OT 機器におけるサイバー脅威の「検知」「対応」「復旧」の対策や教育が早急に必要とされる．

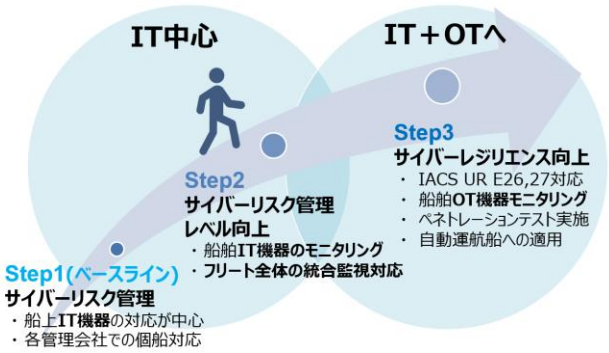

図 9　船舶サイバーセキュリティ対策の道のり

図 9 に示す通り，船舶サイバーセキュリティ対策の道のりにおいて，現状では Step 1 を過ぎたあたりにおり，ベースラインとしてのサイバーリスク管理が船舶運航者を中心として実施されている状況にあるが，今後は Step2 のサイバーリスク管理レベルの向上が必要とされ，さらには Step3 以降では，IACS の統一規則への対応や，自律運航船に代表される船舶の高度自動化などにも対応したサイバーレジリエンス向上の取り組みが必要とされる．

そして，これらの取り組みは，海事業界の各プレーヤが連携して議論して進めていく必要がある．

国内での連携した取り組みとしては，(一財) 日本舶用工業会の「スマートナビゲーションシステム研究会(SSAP)」において，船舶サイバーセキュリティ対策についての情報共有や対策検討，関連する機器の国際標準化などが実施されており，こういった業界横断の連携など通じて，日本においても海事産業全体のサイバーセキュリティ対策レベルが向上していくことを期待する．

参考文献

1) 柴田，三村，安藤，船舶データ収集プラットフォーム SIMS とデータ活用の取り組み，日本マリンエンジニアリング学会誌,第 54 巻 第 2 号(2019)，121-125.

2) 柴田，牧山，安藤，船舶運航とサイバーセキュリティ対策，日本船舶海洋工学会誌，第 91 号(2020)，20-25.

3) IMO,MSC FAL.1/Circ.3「Guidelines On Maritime Cyber Risk Management」，https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf，(参照日 2023 年 2 月 1 日)．

4) IMO,RES.MSC.428(98) 「MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS」，https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution MSC.428(98).pdf，(参照 2023 年 2 月 1 日)．

5) IACS, No.166 Recommendation on Cyber Resilience, https://iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr2-cln/ (参照 2023 年 2 月 1 日)．

6) IACS,UR E26 Cyber resilience of ships，https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_new_apr_2022.pdf，(参照 2023 年 2 月 1 日)．

7) IACS,UR E27 Cyber resilience of on-board systems and equipment, https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e27_new_apr_2022.pdf，(参照 2023 年 2 月 1 日)．

8) NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (参照 2023 年 2 月 1 日)．

9) ClassNK,船上機器システムにおけるサイバーリスク対策検討のためのペネトレーションテスト成果報告書, https://www.classnk.or.jp/hp/pdf/press/report/202007j.pdf (参照 2023 年 2 月 1 日)．