［新たなモビリティ時代のサイバーセキュリティ―セキュリティによるジャパン・ブランドの向上に向けて―］

⑤ 海事産業におけるサイバーセキュリティ対策動向

稗方和夫 東京大学大学院新領域創成科学研究科

海事産業のサイバーシステム化

海事産業とは

海事産業でもサイバーセキュリティは，近年きわめて重要な課題となっている[1]．本稿で海事におけるサイバーセキュリティについて述べるにあたり，海事産業の基礎的構成について説明する．海事産業という言葉には統一的な定義はないが，本稿では造船業や海運業など，海に携わる産業全般を指すこととし，造船会社，海運会社，船級協会，舶用機器メーカ等を中心とした関連産業で構成される．また，その任務は海上貨物輸送であるが，その大きな分類として，国際貨物輸送に用いられる外航船と，国内貨物輸送に用いられる内航船が存在する．外航船と内航船は満たすべき制約や規則が異なるが，本稿では国際輸送に用いられ，国際条約を満たす必要がある外航船を想定して海事産業，海上貨物輸送の基礎的な情報を説明する．

国際条約と IMO

外航船は国際条約に従った運航を行う義務があるが，これらの海事産業に関する国際条約は国連の下部組織である IMO（国際海事機関）により策定される．IMO による代表的な条約には SOLAS 条約（海上人命安全条約）や MARPOL 条約（海洋汚染防止条約）などがある．IMO は国際条約により船舶が満たすべきゴールや機能要件などの基本事項について合意形成を行うものである．

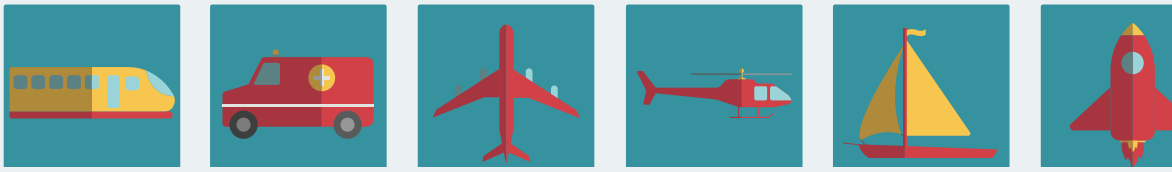
船級協会

IMO により国際条約が策定されると，船級協会という組織がこれらの国際条約や船籍国の国内規則に基づいて船舶を検査し，認証する業務を担う．船級協会は，より具体的には，船体や機関その他の設備に関する基準を定め，基準を満たした船舶を承認している．世界の主要海運国では，中立的な立場で船舶を検査し船舶の等級付けを行うために船級協会を組織している．

歴史ある組織としては英国のロイド船級協会があり，その創設は 1760 年である．日本では 1899 年に設立された日本海事協会が，船級協会としての業務を行っている．日本海事協会は船体構造などの船舶工学に基づく安全性評価などに高い専門性を持つ組織であるが，海洋における安全を確保するための認証機関という組織が持つミッションから，サイバーセキュリティへの取り組みの基本方針や各種のガイドラインの策定と公表を積極的に行っている．船舶運航の安全確保を目的として 2019 年 3 月に発行されたガイドラインであるサイバーセキュリティマネジメントシステム（CSMS）などについては，同年 12 月に初の認証事例もあり，積極的にサイバーセキュリティ対策を進めている．船舶運航の安全確保という目的は変わらず，サイバーセキュリティという新しい技術分野への展開が進みつつある．

造船業と海運業

現在世界には，ばら積乾貨物船，オイルタンカー，コンテナ船，旅客船・RORO 船等，液化ガス船，ケミカル船などの種類の船舶 11 万隻程度が運航されており，その需要，船腹数は毎年 3％伸びている．なお，日本は世界の 10％程度の船舶を運航している．海運



会社は荷主からの要求に応じて貨物輸送を行う．

造船業は海運会社や船主から要求される仕様に応じた船舶を建造し，引き渡す．船級協会からのサイバーセキュリティについての認証を取得するのは船舶のオーナーである海運会社であるため，造船所の立場としては海運会社からサイバーセキュリティに対応した船舶の要求があった際に，サイバーレジリアントな製品としての船舶を建造し，提供するという役割が期待されている．

海事産業のステークホルダの役割

海事産業において，海運会社は，IMO が策定した国際条約を船級協会などと協力して満たしながら，造船所が建造した船舶を保有あるいはチャーターして，海上貨物輸送を行っている．

サイバーセキュリティへの対策をどのように海上輸送に実装するかを検討する上では，船舶の建造している造船会社やユーザである海運会社だけでなく，IMO や各国の船級協会，舶用工業またその他の業界団体の動向も重要となっている．筆者が海上貨物輸送システムを取り巻くステークホルダ間の関係を記述した図を以下の図 -1 に示す．四角はステークホルダで，矢印はステークホルダ間に発生している価値の流れを示している．

海事産業へのサイバーセキュリティ対策の実装では，これらのステークホルダ間の関係を考慮する必要がある．

国内の技術動向：船舶のサイバーシステム化

国土交通省の動向：IoT 活用船 [2)]

近年，海上ブロードバンド通信の進展や情報通信技術を活用した船舶の運航支援技術の高度化に伴い，安全かつ効率的な運航を可能とする自動運航船の導入に向けた動きが活発化している．

日本では，2017 年 4 月の海上運送法の改正により運送サービスの質を向上させる「先進船舶」の研究開発，製造または導入を行う事業者への支援を行っている．「先進船舶」には，燃料を重油から LNG 等に切り替えた「代替燃料船」と，IoT 活用技術を導入した「IoT 活用船」がある．ここではサイバーセキュリティとの関連が深い IoT 活用船について説明する．元々船舶に搭載されている舶用機器は独立に設置され，メンテナンスや運用に必要と

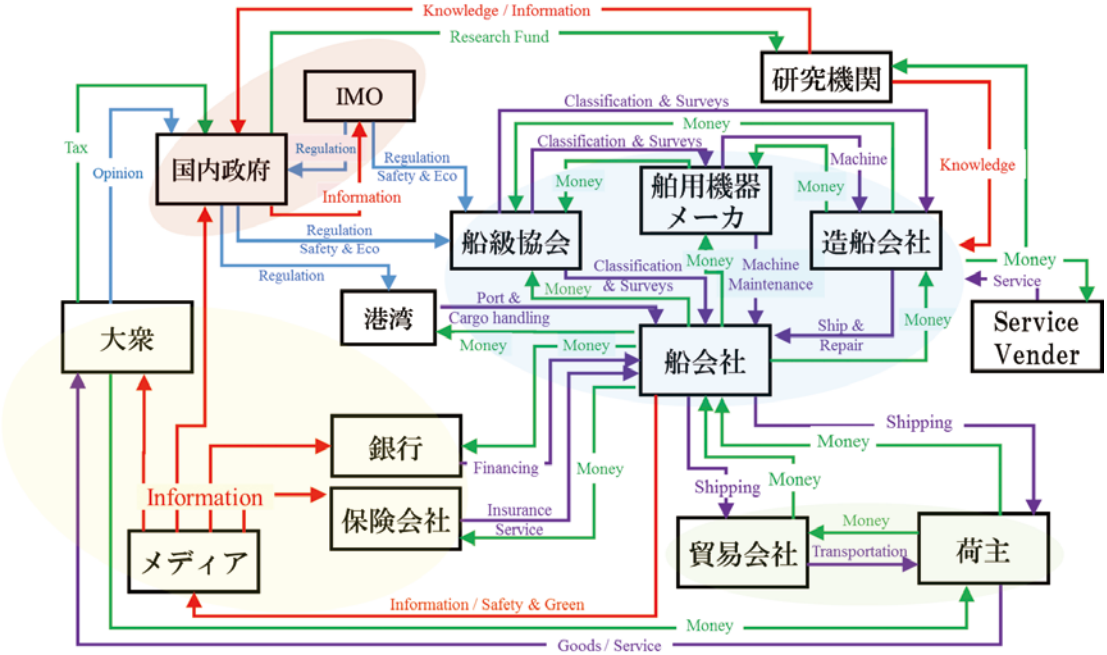


図 -1　海事産業のステークホルダ間の関係

なるデータもそれぞれの機器および機器メーカのみが利用する形式であった．また，航海中のネットワーク接続も限定的であるため，リアルタイムでデータ収集，分析，対処を行うようなことは困難であり，構想は存在しても実証等もあまり行われてこなかった．現在では，海上でのブロードバンド通信の高度化により，他産業と同様に船舶に搭載された機器類の接続やデータ共有が進んでおり，船舶のディジタルツイン開発に向けた研究開発プロジェクトなど，船舶運航の効率化，高度化がIoT活用船のコンセプトに対応する段階に到達しつつある．

自動運航船

IoT活用船に加えて，サイバーセキュリティに関連して話題に上る技術コンセプトとして，自動運航船があげられる．注目を集めている自動運航船であるが，国内外で広く共有される認識や定義はまだ固まっていない．また，自動運航は無人化を想定しているのか，無人化を進める場合にも自律運航を導入するのか，遠隔操船を前提とした運航を行うのかによって，機器類の自動化に要求される水準などは大きく異なると考えられる．一方で，現時点では自動運航がどのように実現されるかといったビジョンはまだ明確になってはいない．このように技術開発の動向としては不確実性の高い状況にあるが，船舶の見張りや機器のモニタリング，操船，機器の制御，離着桟，荷役やその他のタスクの情報技術による支援を行うための研究開発は活発に行われている．自動運航船のビジョンについての不確実性が存在するが，自動運航船とはこれらの業務について情報技術を用いた高度な支援が実現されている船舶を指す言葉と理解することがよいと考えられ，サイバーセキュリティ対策が必須となる技術開発動向である．

海事オープンプラットフォーム化[3)]

概要

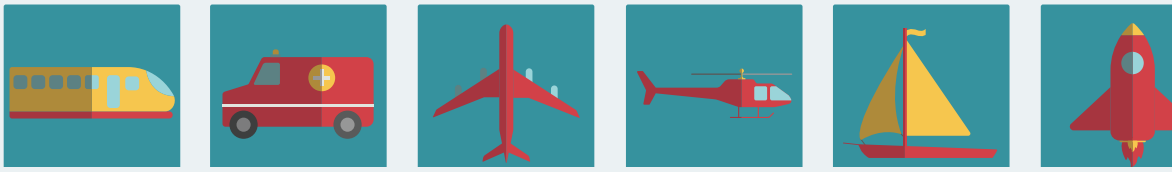
現在の船上の機器は前述のように個別に情報やデータを収集・管理しており，複数の機器から得られるデータを統合することで新たな価値を生むようなアプリケーションを開発するには，実状に合わせて各機器のベンダおよび船主などにデータの開示を交渉し，データフォーマットなどの技術面の調整の両方を経る必要があった．

このような現状から，船上にデータサーバを設置し，標準化されたデータ形式やプロトコルによって各機器のデータを集中管理するという提案が海事産業内ではなされている．この船上データサーバと陸上のデータセンタにおいても標準化されたフォーマットでデータ共有し，また，データ利用の目的に応じてデータ利用の可否やアクセス権限をコントロールする仕組みも合わせて提供するという海事のオープンプラットフォームが提案され，IoS-OP（Internet of Ships Open Platform）として活動を開始している．IoS-OPにはデータ流通にかかわるルールの策定，整備，データ活用の範囲や権利の検討などを行うコンソーシアムもあり，積極的なデータ活用を進めようとしている．

スマートシップに関する国際規格

オープンプラットフォーム化を進めるにあたり，海事産業では日本が主導して2つの規格を策定した．これは，ISO 19847「実海域データ共有化のための船内データサーバ―一般要件」およびISO 19848「船上機械および機器用データ標準」であり，前項のオープンプラットフォームで必要となるデータサーバおよび機器間の通信の標準化を進める上で必須の規格である．今後の舶用機器の利用では，これらの規格に基づいて開発された個々の機器をデータサーバを介したシステム統合を行い，個別機器の開発は分散的でもシステム全体としての機能は統合的に提供できるような仕組みが期待できる．

一方で，データや機器間のコネクティビティがさらに高まることも考えられ，サイバーセキュリティの重要性もまたさらに高まっている．



海事産業のサイバーセキュリティ

海事サイバーセキュリティ検討プロジェクト [4)]

背景

世界的な情報技術の発達に伴い，船舶，港湾，陸上施設などさまざまな海事分野においてもサイバーシステムへの接続および依存が進み，悪意ある団体や個人によるシステムデータへの不正アクセス等に起因する航行安全侵害や，経済的被害等のさまざまなリスクが懸念となっている．このため，2015 年 6 月に開催された IMO の MSC（海上安全委員会）95 において，海事セクターのサイバーセキュリティに関する任意ガイドラインを作成することが合意された．また，米国提案に基づき，海事の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）が採択された．これにより，船主および運航者は，2021 年 1 月 1 日以降の最初の適合証書（DOC）の年次検査までに国際安全管理コード（ISM コード）に基づく安全管理システムを通じてサイバーリスク管理を実施することが推奨されることとなった．

海事サイバーセキュリティ検討プロジェクトの詳細 [1)]

前述のような国際動向を反映して，日本の海事産業においても海事のサイバーセキュリティに関する審議が本格化し，サイバーセキュリティ対策に向けた検討体制の必要性が高まり，産学官公の連携で，海事分野におけるサイバーセキュリティ対策の推進を行うこととなった．日本財団の支援を受け，船舶のオーナおよびユーザを中心とした日本船主協会，製品としての船舶を建造する造船所からなる日本造船工業会および日本中小型造船工業会，船舶に搭載される舶用機器メーカの日本舶用工業会，日本の船級協会である日本海事協会，このほか大学研究機関や公的機関である東京大学，海上・港湾・航空技術研究所 海上技術安全研究所，国土交通省，情報処理推進機構，情報通信研究機構，といった横断型の組織を日本船舶技術研究協会が取りまとめ，「我が国の実態を踏まえて IMO で行われるガイドラインの審議等に貢献すること」，「我が国の海事分野におけるサイバーセキュリティに関する現状を分析し，我が国海事業界に即したセキュリティ対策案を検討すること」の 2 点を目的としたプロジェクトを立ち上げた．

このプロジェクトの活動を通じて，いくつかの成果が出てきている．1 つ目の成果は，IMO におけるガイドライン策定への対応であり，ガイドライン案を米国やカナダ等と共同提案したとともに，ガイドラインの策定に貢献した．2 つ目の成果は安全管理システム（SMS）マニュアルのテンプレート作成である．2021 年 1 月 1 日以降の安全管理システムの適合証書の年次検査までに，サイバーセキュリティ管理を国際安全管理コードに基づく船舶安全管理システムに統合するために，検討すべき項目をまとめたテンプレートを作成した．国際安全管理コードは SOLAS 条約（海上人命安全条約）の中で定められており，安全管理システムの確立などを義務付けている．従来から安全管理システムマニュアルの整備は義務付けられているが，その内容にサイバーセキュリティのリスク管理が要求され始めた．なお，このテンプレートの作成の際には，日本海事協会だけでなく海運の主要国の船級協会によるレビューも実施し，各国の意向やインプットも取り込んでいる．

国際動向

BIMCO（ボルチック国際海運協議会）

日本海運集会所の Web ページ等の情報によると，BIMCO（ボルチック国際海運協議会）は 1905 年に発足の“The Baltic and White Sea Conference”が前身であり，船舶代理店を含むブローカーのほか，PI 保険等を含む「クラブメンバ」や船級協会や海事法律事務所，損保や銀行等海運に関心のある「準メンバ」により構成されている．BIMCO は傭船の契約書書式の標準化などの事業や IMO への働きか

けを行うほか，外航海運に関するデータや情報を発信している．

BIMCO は船内システムおよびネットワークへの無許可アクセス，または悪意ある攻撃リスク等のサイバー脅威が近年大きくなっていることを受け，これらのリスク回避，もしくは低減に向けて，2016 年 1 月にインダストリーガイドライン「THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS」を発行した．本ガイドラインは，船主および運航会社がサイバーシステムのセキュリティを維持できるように，業務評価方法および必要な手順と処置の実行方法を提示するものである．このガイドラインは，2017 年には第 2 版，2018 年に第 3 版が発行されている．第 3 版では IT（情報システム）と OT（装置のオペレーションを高度化する技術であるオペレーショナル・テクノロジー）の違いの明示や，OT へのインシデントでは物理的損傷に結び付く可能性が高いなどの船舶固有の特性に配慮した評価項目を追加している．

国際船級協会連合（IACS）

各国の船級協会の連合体である IACS では，サイバーシステムパネルを設置して IT/OT システムへの技術的なアプローチにより 12 のレコメンデーションを策定した．

米国沿岸警備隊（USCG）と米国船級協会（ABS）

船舶は船籍を持つ国における安全管理システムの審査や，寄航国における検査を受ける必要がある．どの水準のサイバーセキュリティ対策を行うかという観点から，サイバーセキュリティ対策への要求が高いと考えられる米国沿岸警備隊（USCG）がどういったレベルの対策を求めるかを理解することは重要である．USCG と密に連携して活動していると考えられる米国船級協会（ABS）では，サイバーセキュリティに関するリスクを緩和することを目的としたプログラムが存在し，積極的にサイバーセキュリティの認証を行っている．

今後の取り組み

国際動向のまとめ

IMO は，安全管理システムマニュアルの中でサイバーリスクを扱うことを推奨しており，2021 年 1 月以降は対応が進むと考えられる．このほか，BIMCO による業界主導のガイドラインの改版や，各国の船級協会によるサイバーセキュリティマネジメント認証も活発に行われている．

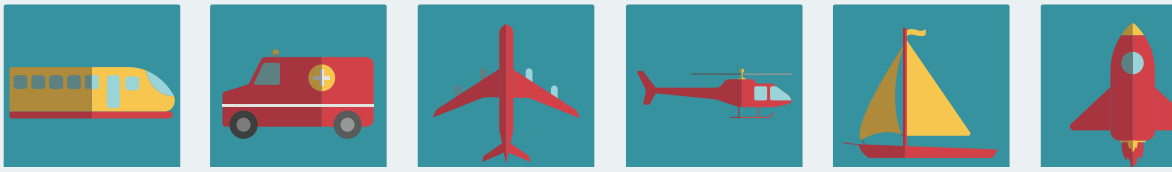
船舶におけるサイバーセキュリティへの取り組み

船舶のサイバーセキュリティ対策を考えるにあたって，大きく分けるとマネジメント的なアプローチと，IT/OT システムへの技術的なアプローチの 2 つがあると多くの組織で考えられている[5), 6)]．

マネジメント的なアプローチとしては，サイバーリスクマネジメント，教育や訓練，ISO 27001（情報セキュリティマネジメントシステム）などによるサイバーセキュリティ対策が想定されている．つまり，組織体としてのサイバーセキュリティへの耐性に取り組むものである．

このアプローチに対して，ソフトウェアアップデート，ネットワークセキュリティ，通信およびインタフェースなどの IT/OT システムへの技術的なアプローチも存在する．こちらは製品としての船舶や舶用機器のサイバーセキュリティへの耐性に取り組むものである．

この 2 つのアプローチに加えて，耐用年数が 15 年から 20 年にわたるという船舶の特徴もあり，マネジメント的なアプローチが必要となるのは運航船のサイバーリスクマネジメントであり，新たに建造する船舶に対してサイバーレジリエントな製品としてシステムインテグレートするというアプローチが有効であろうという共通認識が海事業界内で得られている．関連団体や各種ガイドラインと，運航船および新造船への対応状況を図 -2 にまとめる．多くのインダストリーガイドラインは他産業でも参照されて



いる共通の仕様を海事業界に合わせてカスタマイズしたものであり，図 -2 ではその関係性を分かりやすく図示されている．

今後の海事産業においては，新造船の特に OT 要素がサイバーレジリアント（設計においてサイバーセキュリティ耐性を実現）であることを要求されることが予想され，その対応はシステムインテグレータとしての造船所が担う範囲になると考えられる．一方で運航船および建造後の新造船については，その長い製品ライフサイクルを通じてサイバーレジリアントな状態を保ち，かつサイバーリスクマネジメントが適切になされた運用を行う必要がある．このためには船舶のオーナや海運会社がシステムインテグレータの役割の一環として対応し続けるべきものと考える．

本稿では海事産業におけるサイバーセキュリティを取り巻く国際および国内動向についてまとめた．IT 分野で，あるいはほかの産業ドメインでサイバーセキュリティに取り組んでいらっしゃる方のお役に立つことができれば幸いである．

参考文献

1) 稗方和夫：海事分野におけるサイバーセキュリティ対策に関する取り組み，制御システムセキュリティカンファレンス 2019 講演資料（2019.2.15）．
2) 海事産業の生産性革命の深化のために推進すべき取組について～平成 28 年 6 月 3 日答申のフォローアップ～報告書，国土交通省 交通政策審議会 海事分科会 海事イノベーション部会，2018 年 6 月．
3) 安藤英幸：船舶デジタライゼーション時代に向けた船舶オープンプラットフォームの役割，Sea Japan 2018 展示会 船舶海洋技術セミナー（2018. 4. 13）．
4) 稗方和夫：サイバーセキュリティ検討プロジェクトの活動，日本船舶技術研究協会 船舶基準セミナー～海事サイバーセキュリティへの対応～ 講演資料（2019.7.23）．
5) 柴田隼吾：船舶におけるサイバーセキュリティ対応の現状とこれから，Monohakobi Techno Forum 2019 講演資料（2019.11.25）．
6) 斎藤直樹：船舶におけるサイバーセキュリティ対策の構築へ向けた現況，2018 年度 ClassNK コンサルティングサービスセミナー（2018.11.2）．

（2020 年 1 月 15 日受付）

稗方和夫（正会員） hiekata@edu.k.u-tokyo.ac.jp

東京大学大学院工学系研究科修士修了．日本アイ・ビー・エム（株），東京大学大学院工学系研究科助手等を経て，2010 年より大学院新領域創成科学研究科准教授．博士（工学）．2013 ～ 2014 年 MIT 客員研究員．

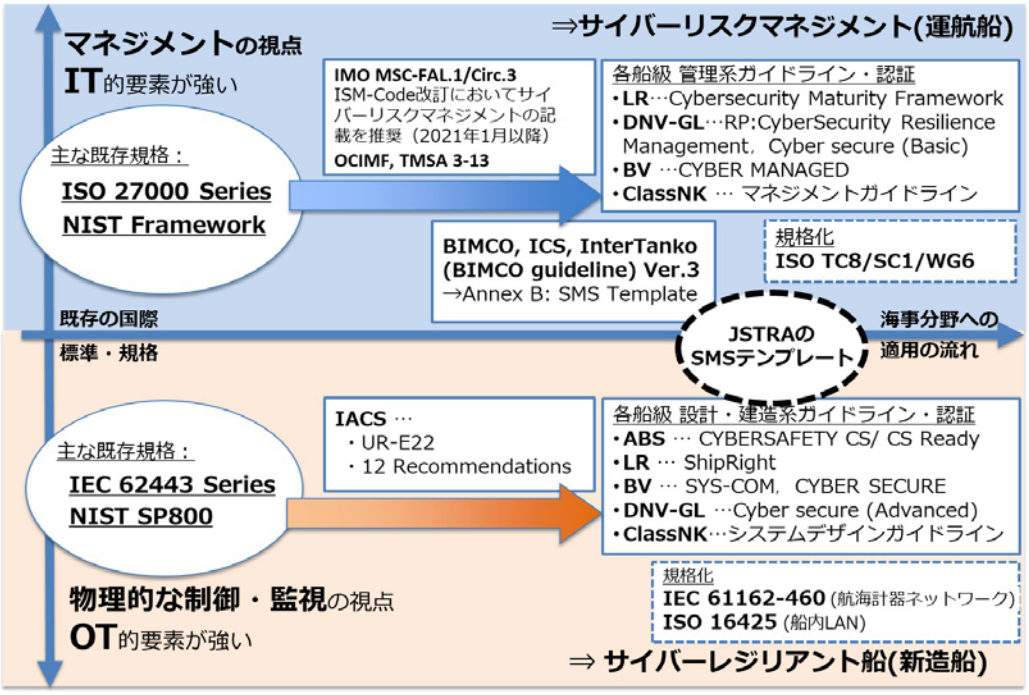


図 -2　新規建造船と運航船のサイバーセキュリティ対策