海事サイバーセキュリティの現状と課題

三石 靖裕[†1] 橋本 正樹[†1] 辻 秀典[†1] 湯淺 墾道[†1]

概要：近年，わが国政府は海事産業の振興と国際競争力の向上のため，海事分野に ICT や IoT 等の技術を導入し，デジタライゼーションを強力に推進しようとしている．2025 年までには自動運航船の実用化も目指しているところであり，サイバーセキュリティの確保は重要な課題である．一方で，海事分野でのサイバーセキュリティについては，未だ十分な研究がなされているとは言い難く，特に我が国については，現状整理と課題抽出の段階にあると言えよう．本研究は，我が国の海事サイバーセキュリティの現状と課題について，網羅的・体系的な整理を試みることで，今後の海事サイバーセキュリティの発展に資することを目的とするものである．

キーワード：海事サイバーセキュリティ，自動運航船，重要インフラ，海運，GPS

Current Status and Issues of Maritime Cyber Security

Yasuhiro Mitsuishi[†1] Masaki Hashimoto[†1] Hidenori Tsuji[†1] Harumichi Yuasa[†1]

Abstract: In recent years, to promote the maritime industry and improve international competitiveness, the Japanese government intends to strongly promote digitalization by introducing technologies such as ICT in the maritime field. Cyber security is an important issue. Meanwhile, sufficient research has not been done yet on cyber security in the maritime field, and especially Japan is at the stage of current status summarization and problem extraction. This work aims to contribute to the development of maritime cyber security in the future by attempting to comprehensively and systematically organize the current status and problems of maritime cyber security in our country.

Keywords: Maritime Cyber Security, Autonomous Ship, Critical Infrastructure, Maritime Transportation, Global Positioning System

1. はじめに

サイバー空間は今や欠くことのできない社会基盤になっており，陸上，海上，航空，宇宙の区別なく拡がっている．我が国は四方を海で囲まれた島国である．日本の国土面積約 38 万平方 km に対し，領海，内水，排他的経済水域等を含む管轄海域面積は約 465 万平方 km に及び，これは国土面積の約 12 倍に達する．[1]また，我々が生活するうえで必要な資源，エネルギー，食糧等の輸送は海上輸送が主である．2016 年の国際航空貨物輸送量 159 万 3,272 トンに対し海上輸送量は 9 億 3,522 万トンに達し，わが国の国外との物流は海上輸送に大きく依存している状況である．[2][3]また，我々が日常利用するインターネットを始めとする情報通信分野においても，国外との通信は地球上の各大陸を結んでいる海底ケーブル[4]が主でありこの分野でも海が重要な領域になっている．これらを支える海事産業はわが国の重要インフラと言えよう．

わが国の海事産業の中核となる造船業は 1956 年以降ほぼ半世紀にわたり船舶建造量世界シェアトップを維持していたものの，1980 年代には韓国が，1990 年代には中国の船舶建造量が増加し，現在日本のシェアは約 2 割程度まで低下している．また，造船業の課題として団塊の世代の大量退職によるベテラン造船業技術者の減少のため技術力の低下もあり，生産性の低下要因となっている．

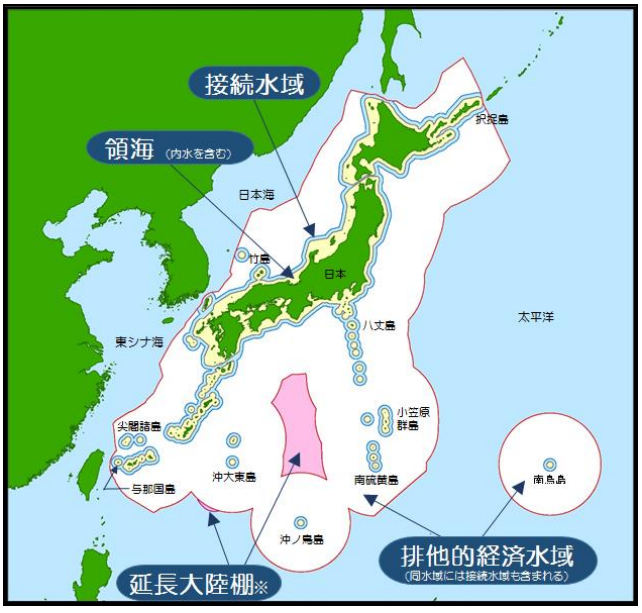

図 1 日本の領海等概念図[1]

わが国政府は ICT を活用することにより，このような問題を始めとした海事産業の課題解決に取り組み，生産性，国際競争力の向上を目指している．[5]今後，海事産業分野

†1 情報セキュリティ大学院大学
Institute of Information Security

i 筆者による邦訳

への ICT の導入がこれまで以上に促進されることが予想され，海事分野においても業務の省力化，効率化向上のため IT への依存は高まっていく状況にある．それにつれサイバーセキュリティ確保の重要性も高まっていくと考えられる．

海事産業について，未だ国内で重大な被害をもたらしたサイバー攻撃事例は見られないものの，今後サイバー攻撃により海事産業に重大な被害が発生すれば，我々の社会生活に多大な影響を与えることとなるため，この分野でのサイバーセキュリティの重要性は日々高まっており，注目すべきものとなっている．

1.1 本研究のねらい

まず，本研究は海事サイバーセキュリティの研究動向（特に船舶を中心としたサイバーセキュリティ）について研究するものであることを明記しておく．

先に述べたようにわが国海事分野への ICT の導入が進み，造船業を始め建造される船舶，船舶の運航に関連する産業，港湾施設，海運業等関連する産業間がネットワークを介し日々のサービスを提供するようになってきた．

また，大容量通信の可能な通信衛星の実用化により，洋上の船舶も陸上の通信環境に近づいており，インターネットへ常時接続される船舶も出てきている．通信環境の向上と共に政府は内閣が発表した“未来投資戦略 2017” で造船，海運の国際競争力強化のため，2025 年までに自動運航船の実用化を目指すとしている．陸上と常時船舶がネットワークで繋がるようになり，我々が日常生活を送る陸上と同様にサイバーセキュリティが確保されなければこれらサービスの安全は維持できなくなってきた．

海事分野におけるサイバーセキュリティについて国内で発表された論文はほとんど見られず，研究は十分であるとは言い難い状況である．本研究では海事サイバーセキュリティの現状を網羅的・体系的に整理し，課題を抽出することで本研究分野の発展とわが国海事サイバーセキュリティの発展に寄与したい．

1.2 本稿の構成

本稿では，海事サイバーセキュリティについて一般的なサイバーセキュリティとの比較をし，海事サイバーセキュリティの特徴等を述べる．次に海事サイバーセキュリティを取り巻く情勢について諸外国，わが国について述べる．

海事サイバーセキュリティに関する諸研究について示した上で現状の課題等考察を述べて，今後の研究方針を示す．

2. 海事サイバーセキュリティについて

2.1 海事産業とデジタライゼーション

海事産業とは主に船舶に関連する産業，「造船業」，「海運業」，「港湾運送業」等で構成される中核的海事産業，「損害保険」，「倉庫・物流」，「商社」等で構成される中核的海事産業以外のその他多くの産業が集合し，海事産業クラスターといわれる産業の集合を形成している．[6]

日本政府はわが国の海洋に関する諸政策を海洋基本法及び海洋基本計画に基づき推進している．海洋基本計画はおおむね 5 年ごとに見直しを行っているところ，平成 30 年 5 月 15 日に第 3 期海洋基本計画を閣議決定している．その中で「高付加価値化・生産性の向上を通じて，海洋産業の国際競争力を強化」する旨示されている．[7]

図 2　海事産業[6]

海事産業の生産性向上等のために導入が推進されているのが，ICT を始めとする技術によるデジタライゼーションである．海上ブロードバンド通信の普及，人工知能研究の進展等デジタル技術の発展に見られる技術革新により，具体的には船舶の開発・建造・運航に至る全てのフェーズでこれらの技術を取り入れるもので，開発・設計に数値シミュレーションを用いる，造船所における IoT を活用した工場の見える化システムの実証試験，船舶運航に IoT を導入し陸上から船舶の様々なデータを収集することで，航行支援，機関故障予測による稼働率の向上等が期待されている．

また，航行中の船舶から収集した航行データをビッグデータとして活用する動きもある．[8][9][10]例えば，実際に航行する船の船体にかかる応力データを船舶設計・開発にフィードバックし船体設計の最適化に活用するといったことが可能となる．これら技術により海事産業の国際競争力強化を目指すものである．現在，国土交通省海事局が進めている一連のデジタライゼーションの施策を「i-Shipping」と呼んでいる．[5][11]

2.2 船舶の特徴

海事サイバーセキュリティについて論じる上で，海事産業の中核を成す船舶の特徴について理解しておく必要があるだろう．なお，本稿では主に海外航路で運航されるような大型船舶を対象として論じることとする．

船舶の特徴としては，

① 水上を移動する（乗り物としての船）

② 小型のものから非常に大きなものもある（大型原油タンカーは全長 300m，全幅 60m を超える船

舶もある．[12]巨大構造物としての船）

③ 推進用機関の他発電機やポンプ類の補機を持ち，24 時間稼働のプラントとしての側面，乗員や客船では乗客の居住設備を備え移動する建造物としての側面も持つ（プラント，構造物としての船）

④ 大量輸送が可能（大型原油タンカーでは約 30 万トン，ドラム缶約 150 万本分を積載[12]，大型クルーズ客船では旅客数 4,000 人を超える[13]，大量輸送手段としての船）かつ様々なモノを運び，その中には危険物（可燃性，毒性を有する貨物もある）

⑤ 建造から廃船までのライフサイクルが長い（30 年以上運航される場合もある）ため，旧式化したシステムが更新されないまま稼働している，また，仕様上ソフトウェアのアップデートやセキュリティパッチの適用ができないものが存在する．

⑥ 航行中は洋上で孤立している（トラブルの初動対応は乗員で行う，陸上のサポートは限定的となる）

⑦ 長大なサプライチェーンを有する

船舶はこのような特殊性を有している．そして，日々わが国周辺海域や港湾を多数の船舶が航行，出入港しているのである．

2.3 船舶搭載システムの脆弱性

先に述べたように船舶は乗り物としての構造，プラントとしての構造を持ち合わせてそれがシステムとして機能している．そこへ近年 ICT の導入を始めとしたデジタライゼーションの波が押し寄せている．船舶運航の効率化，安全性の向上のため ICT の依存度が高まり，陸上と同様 ICT の安全な運用にはサイバーセキュリティの確保が欠かせず，事故が人命の喪失に直結する船舶の場合は安全性への配慮がより必要になろう．ここで，船舶搭載システムではサイバーセキュリティを考える上でどのような脆弱性があるのか触れておく．

Denis ら[14]によれば，脆弱性を懸念する船舶システムとして以下を挙げている．

① IT ネットワーク

② 産業制御システム（ICS: Industrial Control Systems）

③ 自動船舶識別装置（AIS: Automatic Identification System）

④ 電子海図情報表示装置（ECDIS: Electronic Chart Display Information System）

⑤ 超小型衛星通信システム[i]（VSAT: Very Small Aperture Terminal）

⑥ GPS（Global Positioning System）

IT ネットワークは荷役･積荷管理，通関手続，人事管理，データベースによる情報等，業務の基幹となる部分で使用されており，その依存度は高まっている．IT ネットワークではソフトウェアを最新に保つ，セキュリティパッチを適時適用する，重要なシステムはセキュアな場所に設置し適切なアクセスコントロールを実施する等の対策を講じておく必要があり，対策が不十分な場合マルウェア感染によるシステムの停止，それによる船舶運航の阻害のおそれがある．

ICS（産業制御システム）は主機関，補機（発電機，ポンプ等）類の制御や温度，圧力，電圧のモニター等に使用され，ヒューマンエラーの減少，オペレーションの効率化，機器の長寿命化等に貢献している．

これらの機器類は異なるベンダーにより製造された物，異なる技術世代の物，異なるプロトコルで動作する物が混在していること，多くのコンポーネントがセキュリティを考慮した設計，プログラムになっておらず，データを平文で交換する仕様になっている．これらが脆弱性となっている．

これら ICS が IT ネットワークと接続されることで船舶機器類のデータ（温度，圧力等）を陸上施設からモニターすることが可能になり，故障の早期発見，障害対応，現地出張コストの削減等が可能となったが，同時に攻撃者に対して攻撃の入り口を与えることになった．

AIS とは Automatic Identification System，船舶自動識別装置のことであり，船舶と陸上施設または船舶間で使用される装置で，船舶の船名・位置・針路・船速および行先・到着時刻などの情報を相互に交換できる．船舶交通管制，海難捜索救助，事故調査，気象予報の放送等に活用され，船舶の衝突や乗揚げ防止に活用されている．AIS 送受信機はこれらの情報をいかなる認証，完全性チェックが行われることなく VHF で送信している．

図 3 AIS の表示例[15]

i 筆者による邦訳

そのため攻撃者はソフトウェア無線を用い，虚偽の気象予報等誤った情報を送信することができ，船舶の衝突や乗揚げ等を引き起こすことも可能である．[16]

ECDIS は Electronic Chart Display Information System，電子海図情報表示装置といい，ディスプレイ上に海図を表示し，航路の作成や航海に必要な情報を表示するなどする装置であり，国際海事機関により搭載が義務化[ii]されていることから多くの船舶で使用されている．ECDIS のソフトウェア実装には広範な脆弱性が指摘されている．しばしば ECDIS が旧式コンピュータ（例えば OS が Windows XP）上で稼働しており，セキュリティアップデートが未実施である．電子海図はデータの更新を行い最新の状態にしておく必要があるが，インターネットまたは USB メモリ，DVD メディアを介し行う必要があり，セキュリティアップデートがされていない場合マルウェア感染のリスクがあり，結果として船舶衝突や乗揚げなどの重大な結果をもたらすおそれがある．

図 4 ECDIS[17]

VSAT は Very Small Aperture Terminal，超小型衛星通信システムといい，船舶に小型の衛星通信設備を設置して行う．海上においても高速な通信（1Mbps 以上）[18]が可能となる．洋上でも常時接続のインターネット環境を得ることができ，近年は船舶に設置されている種々のシステムが VSAT を経由し陸上とデータ交換をするようになってきた．先述している IT ネットワークや ICS 等も接続されるが，これらに脆弱性がある場合遠隔からサイバー攻撃を受けるおそれがある．また，VSAT 端末の管理画面へはブラウザを使用し接続できるが，設定に不備があると外部から管理画面へアクセスできるおそれがある．さらに管理画面へのログイン情報がデフォルトのままだと VSAT の機種が判明している場合，製品情報から初期ユーザネーム，パスワードを知った攻撃者が不正にログインして VSAT 経由で船舶システムにアクセスされる危険がある．検索エンジン「SHODAN[iii]」で VSAT を検索すると，外部に公開されてしまっている VSAT の IP アドレスが検索でき，管理画面へアクセスできた場合先述のような攻撃をうけるおそれがある．[19][20]

図 5 VSAT ログイン画面[19]

GPS は船舶搭載システムを構成する種々の機器類へ位置情報を提供しており，航海に必須の機器となっている．この GPS についても脆弱性が指摘されている．GPS 衛星が送信する信号は認証，完全性チェックの仕組みがなくなりすまし，改ざんが可能であること，衛星の送信する信号は強度が弱くジャミングによる妨害が可能である．[21][22][23]

また，GPS，AIS，ECDIS，オートパイロット等の航海計器同士が情報の送受を行うプロトコルは NMEA0183[iv]が従来から用いられている．このプロトコルはデータを平文テキストの形式で扱うもので，認証，暗号化といった仕組みがないため盗聴，改ざんの危険があり，オートパイロットに送られるデータが改ざんされた場合，最悪のケースでは船舶が衝突や乗揚げ事故を起こすおそれがある．[20]

2.4 自動運航船

海事サイバーセキュリティが重要な要件となるのが自動運航船ではないだろうか．船舶の自動化については，自動化のレベルにより有人による運航の省力化，効率化，安全性の向上を図るものから，完全無人で船舶を自律運航させるものまでがある．現在，自律運航船を目指す研究・開発に海外でも取り組んでおり[24][25][26]，ノルウェーでは世界初となる自律コンテナ船を建造し，2019 年にも実際に海上での操船試験を開始するとのことである．[27]わが国も海洋基本計画[7]や未来投資戦略[28]等で国の重要政策として 2025 年までの実用化をめざしている．

ii 筆者注：わが国では法令（船舶設備規程）により総トン数 500 トン以上 3,000 トン未満の旅客船及び総トン数 3,000 トン以上の船舶であって国際航海に従事する船舶に搭載義務がある

iii SHODAN：http://www.shodanhq.com/

iv NMEA 0183 Standard：https://www.nmea.org/content/nmea_standards/nmea_0183_v_410.asp

図 6 自律コンテナ船（完成予想図）[27]

国内では平成 29 年度から国土交通省の支援による産官学の研究プロジェクト「自律型海上輸送システムの技術コンセプトの開発」が始まっており，船舶の自動化レベルの定義に基づいた自律船コンセプトを策定，自律船実現に必要な開発要素を洗い出し，自律船実現のためのロードマップを整備することを目指している．

このように各国で自動運航船の研究・開発が進行しているところ，船舶の自動運航について自動化，自律化の定義，が定まっておらず，自動運航船に関するガイドラインの作成，改正すべき国際条約，国内法等の洗い出しなど解決すべき課題は技術的なもの以外にも山積しているといえよう．そして，自動運航船の実用化，安全性にサイバーセキュリティの確保は重要な要素である．海外では自動運航船のサイバーセキュリティを扱っている研究[29][30]も見られる．国内でも論文は散見され，関心の高さが伺える[31][32]．自動運航船の法的な取り扱いに関するもの[33][34][35][36]，自律運航を実現するための技術[37]についてなどで，国内研究でサイバーセキュリティを扱っているものは見られなかった．自動運航船のサイバーセキュリティについては今後の動向を注視したい．

2.5 海事サイバーセキュリティの特徴

海事サイバーセキュリティの特徴について考えてみる．海事サイバーセキュリティが一般的なサイバーセキュリティと異なる点は，大きい点ではインフラが陸上と海上に分かれているところにあり，さらに陸上のインフラも港湾，荷役施設，航行管制施設，造船所等に分けられる．海上の船舶内では IT ネットワーク，GPS，AIS，ECDIS，ICS，VSAT 等のシステムが稼働しており，それらが陸上と VSAT を経由してデータの送受信をしている．先述のとおり，未だサイバーセキュリティ上のリスクを抱える船内システムがネットワークで陸上と接続されているのが，現状の海事サイバーセキュリティの特徴といえる。

今後，船陸間の通信が今以上に行われるようになり，船舶の置かれる環境はよりサイバーセキュリティを意識せざるを得ないものとなっていくだろう．

図 7 海事サイバーセキュリティの対象イメージ

また，船舶を運航する船員の問題もある．外航船員の国籍は様々であり，それら船員の IT リテラシーも様々である．今までサイバーセキュリティについて教育を受ける機会も少ないか全くなかったことが考えられ，今後船舶の IT 化が進めば，船員に対してもサイバーセキュリティの知識付与が重要となってくるだろう．海事産業は国を跨いで広範囲な産業といえる点も特徴といえる．

3. 海事サイバーセキュリティを取り巻く情勢

3.1 諸外国の状況

3.1.1 国際海事機関

IMO は海事サイバーセキュリティについて，2016 年 5 月「海事サイバーリスクマネジメントに関する暫定ガイドライン」[38]を公表している．このガイドラインでは海事インフラにおいて様々なシステムが不可欠であること，それらが相互に接続されて使用されていることについてサイバーリスクがあるとされている．海事インフラでは IT システムと物理プロセスの制御，監視に使用される OT システムが使用されており，双方の脅威を考慮する必要があるとしている．また，リスクマネジメントのフレームワークには「特定」「保護」「検出」「対応」「回復」の５つの要素を組み込む必要があり，サイバーリスクマネジメントは最高幹部レベルから始める必要があるとしている．

3.1.2 米国

米国ではサイバーセキュリティに対する各省庁の役割について，重要インフラ防護，情報共有を国土安全保障省が，法執行，捜査を司法省が，国防を国防総省がそれぞれ担当している．[39]合衆国沿岸警備隊（USCG）は「UNITED STATES COAST GUARD CYBER STRATEGY」[40]を 2015 年に発表しており，海事重要インフラをサイバー脅威から防護する必要があるとし，「サイバー空間の防御」「可用性の確保」「インフラの防護」を挙げて，USCG のみならず民間海事分野のサイバーセキュリティ確保にも取り組んでいる．

民間分野に対する取り組みとしては，国内の港湾ごとに置かれている関係官庁，事業者で構成される地域港湾安全委

員会において，物理セキュリティとサイバーセキュリティ対策を策定しており，商船関係者には配布資料によりサイバーセキュリティに対する意識付け,教育を実施している．

3.1.3 欧州

欧州ネットワーク情報セキュリティ庁（ENISA）はサイバー脅威が ICT システムに依存するすべての産業に拡がっているとし，ICT の堅牢化を確かなものにする必要があるとしている．[41]

海事サイバーセキュリティへの認識は EU 域内でも低く，EU 加盟国は海運業，港湾当局，サイバーセキュリティ当局等は海事セクターの意識向上キャンペーンやサイバーセキュリティトレーニングの実施を推奨している．

現在の海事関連政策は物理的セキュリティを考慮したものとなっており，政策立案者はサイバーセキュリティの側面を追加するべきとしている．

また，海事セクター内の重要な資産の特定と海事固有のサイバーリスクの評価，包括的なリスクベースのアプローチを強く推奨している．

3.2 我が国の状況

3.2.1 政府

わが国政府の動向として，サイバーセキュリティ戦略本部が定めた「重要インフラの情報セキュリティ対策に係る第４次行動計画」[42]では船舶運航事業，港湾運送事業が重要インフラの物流分野に含まれ，海事産業のごく一部ではあるが，官民が連携し保護すべきインフラとされている．

国土交通省は「物流分野における情報セキュリティ確保に係る安全ガイドライン」[43]を作成し事業者自身が情報セキュリティ対策をするための参考資料として公開している．このガイドラインでは，多くの事業者で，情報セキュリティ対策の継続的改善の実施が不十分という課題認識があることから，PDCA サイクルに沿った情報セキュリティ対策の継続的改善の実施が必要であるとしている．

そのような中で，海事分野への ICT 技術の導入による「海事生産性革命：i-Shipping」[5][11][44]を強力に推進するとしている．これは，船舶の建造から運航にいたるすべてのフェーズに ICT，IoT を取り入れ，造船・海運の競争力向上を図るものである．そして，その先には 2025 年までの自動運航船の実用化を目指している．

このように海事分野の ICT 化は政府主導でますます進んでいくものと思われる．しかし，ICT や IoT 等海事産業のデジタライゼーションを強力に進めていくことを政策にしているものの，これらのテクノロジーを活用するためにはサイバーセキュリティが不可欠であるが，これについては自動運航船に関する施策の文章中にわずかに言及されるのみで，他の施策には明示されていない．海事サイバーセキュリティの確保について施策に明記すべきであろう．

3.2.2 民間

民間分野では（一財）日本船舶技術研究協会が 2016 年度から３カ年の予定で「海事分野におけるサイバーセキュリティ対策に関する研究」[45]を実施している．研究内容は IMO における審議動向を的確に把握し，我が国の知見及び意向を反映させるための研究とされている．

また船舶のデジタライゼーションが進み，船舶の運航データを集積，共有して造船，舶用機器の改良，サービス開発に役立てる基盤「IoS オープンプラットフォーム」も 2018 年 5 月末から始動しており，海事分野の IoT 基盤として今後データを収集する船舶数を 2022 年までに 550 隻とすることを目指している．[46]

このことからも今後「コネクテッド」な船舶の増加が予想でき，それに伴いサイバーセキュリティ上のリスクも高まっていくと考えられる．

4. 海事サイバーセキュリティに関する諸研究

海事サイバーセキュリティ関連研究について，国内での学術論文の発表はほぼ見られず，海外での発表がほとんどという状況である．英国には海事サイバーセキュリティを研究する研究室も存在する．[47]

2.3 で述べた Denis ら[14]の他に船舶システムについて他の研究者[48][49]も GPS，AIS，ECDIS，VSAT，ICS の脆弱性を指摘しており，これらがサイバーセキュリティを考慮した設計になっていないか設定に不備があった場合サイバー攻撃のリスクがあると述べている．攻撃者はターゲットとなる船舶の航路を変更させたり,航行を妨害したりでき，海上輸送の安全性，信頼性に長期的な影響を与え得るとしている．多くの研究者がこれらの問題が指摘しても，海事関係者が深刻に受け止めないことが問題であると述べている．また，サイバー攻撃に備えてバックアップ手段の必要性を訴えている．米海軍では，一時期教えることをやめていた天文航法[v]の教育を GPS が使用不能になった場合に備えて復活させている．[50]船舶の分野は古くからの技術で最新技術のバックアップになり得ることが多い点も特徴として考慮しておく必要があるだろう．裏を返せば，従来技術で不都合を感じない関係者も多いと考えられ，それが海事分野，特に船舶への ICT 導入が陸上より緩やかな理由の一つではないかと考えられる．

海事産業へのサイバー攻撃例については，麻薬密輸目的で貨物輸送関連システムへ侵入し麻薬入りコンテナを犯罪組織が手配したトラックに積み込ませるように操作したベルギーでの事例[51]，自航式海洋掘削プラントのメインシステムが作業員の持ち込んだ USB メモリからマルウェア感染し，掘削システムが停止したメキシコ湾での事例などが紹介されている．海洋掘削プラントでのマルウェア感染

v 天文航法：太陽のような恒星，その他惑星等天体の方位，高度を測定することで地球上での船舶，航空機の位置を特定する航海術

は作業員がポルノ画像入りの USB メモリを業務システムに接続したことが原因となっている．作業員に対するセキュリティ教育や，デバイスの適切なコントロールなど既存の対策で防ぐことができた事例といえる．海事産業のサイバーセキュリティ対策には一般的なサイバーセキュリティ対策をまず適切に実施することで対応できる部分も多いのではないだろうか.

5. 考察

これまで海事サイバーセキュリティについて,海事産業,船舶のデジタライゼーション,船舶搭載システムの脆弱性,自動運航船の状況，国内外の取り組み等を見てきた．日本政府，国内海事産業がサイバーセキュリティの重要性は理解しているように見える.

しかし,個別に見た場合,例えば船舶搭載システムでは,サイバーセキュリティを考慮していない設計が多いことや,舶用機器メーカーの規模によりサイバーセキュリティに取り組む体制が異なり，セキュリティリスクとなっていることが伺える．今後は設計時から各メーカーがセキュリティ対策を考慮した製品を提供し，システムを構築する際にメーカー毎にセキュリティ対策レベルに偏りが生じないよう,業界全体でサイバーセキュリティ対策に取り組むことが求められる．船舶搭載システムは機能が停止すると船舶の航行が困難になるおそれがあるので，バックアップ手段を用意しておく必要がある．それには天文航法のような従来技術が有効である．先端技術の導入は多大な利益をもたらすが，先人の知恵も未だ必要となる場合があることを認識しておく必要があるだろう.

また，海事関係者に対するサイバーセキュリティの知識付与についても今後の課題と言える.船舶において IT 化は進んでいる．従来船舶では船体，機関，計器類は基本的には乗員で整備し，不具合についても可能な範囲で乗員による修理が行われてきた．それは船舶には航海中洋上で孤立するという特殊性があるためで，そのための教育が船舶乗組員である海員に対して行われている．しかし，サイバーセキュリティに関する教育はなく，今後船舶の IT 化，システム化が進めば現行の教育では海員により航海中のサイバーインシデントに対応することは困難である．海員に対してはその特殊性に応じたサイバーセキュリティについての知識，技能の付与が今後必要になってくるのではないだろうか.

海事サイバーセキュリティの研究では国外の研究，取り組みが先行しているといえる．船舶におけるサイバーセキュリティマネジメントフレームワークも海外海事団体で作成され，IMO でもこれを参考にしている．海外では複数論文やレポートが発表されており，海事サイバーセキュリティのカンファレンスも開催されている．翻って我が国は海事産業の国際競争力強化のために積極的にデジタライゼーションを推進し，2025 年までに自動運航船の実用化を目指すなど，先進船舶の開発にも意欲的であるものの，サイバーセキュリティについては政府の施策の中に言及されている部分は限定的であり，開発の推進と温度差を感じるところである．民間分野では（一財）船舶技術研究協会で検討がなされているものの，国内での学術論文の発表もほとんど見られない．今後の研究の発展が期待される.

6. まとめ

海事サイバーセキュリティの現状について調査をしてみると，海外で活発に研究されていることがわかった．それは関連論文の数が国内研究に比べて顕著に多いことからも伺える．可能な限り網羅的に調査をすることとしてきたが，まだ調査していない論文が多くあるため継続して論文の調査，国内外の海事サイバーセキュリティに関する動向や今後の実用化が待たれる自動運航船の研究動向，特に今後どのようにサイバーセキュリティ対策がなされるのか調査していきたい.

我が国は安定した海運が，豊かで安全な国民生活を支えており，シーレーンの確保等安全保障上も海洋の安全確保は重要な問題である．わが国海事産業の発展と海上の安全が維持されるためには，今後この分野の研究が盛んになることが求められる.

参考文献

[1]“海上保安庁海洋情報部 日本の領海等概念図” https://www1.kaiho.mlit.go.jp/JODC/ryokai/ryokai_setsuzoku.html（参照 2018-08-09）

[2] “国土交通省 海事レポート 2017” http://www.mlit.go.jp/common/001193454.pdf（参照 2018-08-09）

[3] “国土交通省 平成 28 年度航空輸送実績について（概況）”

[4]http://www.mlit.go.jp/k-toukei/11/annual/11201600a00000.p-df（参照 2018-08-09）

[5] Submarine cable map https://www.submarinecablemap.com/（参照 2018-08-09）

[6] “国土交通省 交通政策審議会海事分科会 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 30 年 6 月 1 日”， http://www.mlit.go.jp/common/001237394.pdf（参照 2018-06-25）

[7] “日本船主協会 日本の海運 2017-2018” https://www.kaijipr.or.jp/shipping_now/pdf/allpage2017.pdf（参照 2018-08-09）

[8] “内閣 海洋基本計画（平成 30 年 5 月 15 日閣議決定)” http://www8.cao.go.jp/ocean/policies/plan/plan03/pdf/plan03.pdf（参照 2018-08-09）

[9] “日刊工業新聞 2018 年 6 月 13 日” https://newswitch.jp/p/13281（参照 2018-08-09）

[10] 安藤英幸. 海運における IoT とビッグデータの活用 (< 特集> IoT 技術). 日本船舶海洋工学会誌 KANRIN (咸臨), 2016, 64: 12-19.

[11] 池田靖弘. シップデータセンターについて-船舶 IoT 基盤のオープンプラットフォーム化. マリンエンジニアリング, 2017, 52.2: 201-204.

[12] 川村竜児. 先進安全船舶技術研究開発支援制度について-海事産業の生産性革命 「i-Shipping (Operation)」. マリンエンジニアリング, 2017, 52.2: 175-178.

[13] “出光タンカー（株） タンカーを知る” http://www.idemitsu.co.jp/tanker/know/trivia/hull/size.html（参照 2018-08-09）
[14] 池田 良穂．世界の客船の現状：フェリーとクルーズ客船．日本船舶海洋工学会誌 KANRIN（咸臨）．2008, vol.17，p. 2-6
[15] Dennis Bothur. et al. A CRITICAL ANALYSIS OF SECURITY VULNERABILITIES AND COUNTERMEASURES IN A SMART SHIP SYSTEM. 15th Australian Information Security Management Conference. 2017, p. 81-87
[16] “古野電気 （株）「AIS の基礎知識」” https://www.furuno.com/special/jp/ais/technology/#About（参照 2018-08-10）
[17] Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit. A security evaluation of AIS automated identification system. Proceedings of the 30th annual computer security applications conference. ACM, 2014.
[18] https://www.furuno.com/img/prev/jp/markets/merchant/ecdis/FMD-3200_3300/cartography_img_002_l.jpg（参照 2018-08-09）
[19] “総務省「移動衛星通信システムの現状等」” http://www.soumu.go.jp/main_content/000432704.pdf（参照 2018-08-09
[20] “Pentestpartners．OSINT from ship satcoms” https://www.pentestpartners.com/security-blog/osint-from-ship-satcoms/（参照 2018-08-10）
[21] “Pentestpartners． Hacking, tracking, stealing and sinking ships”https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships/（参照 2018-08-10）
[22] Warner, Jon S., and Roger G. Johnston. GPS spoofing countermeasures. Homeland Security Journal. 2003, 25.2 p.19-27
[23] Ruegamer, Alexander, and Dirk Kowalewski. Jamming and Spoofing of GNSS Signals–An Underestimated Risk?!. Proc. Wisdom Ages Challenges Modern World. 2015, p.17-21
[24] Bhatti, Jahshan, and Todd E. Humphreys. Covert control of surface vessels via counterfeit civil GPS signals. University of Texas, unpublished 2014.
[25] “MUNIN”http://www.unmanned-ship.org/munin/（参照 2018-08-15）
[26] “Rolls-Royce AAWA whitepaper”https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf（参照 2018-08-15）
[27] “海上技術安全研究所「海外の自動運航船の技術開発 動向と今後の取り組み」” https://www.nmri.go.jp/_src/4238/17kouen_5.pdf（参照 2018-08-10）
[28] “KONGSBERG 「Autonomous ship project, key facts about YARA Birkeland」” https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/4B8113B707A50A4FC125811D00407045?OpenDocument（参照 2018-08-15）
[29] “内閣「未来投資戦略 2018」” https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_zentai.pdf（参照 2018-08-10）
[30] TAM, Kimberly; JONES, Kevin. Cyber-Risk Assessment for Autonomous Ships. 2018.
[31] TAM, Kimberly; JONES, Kevin. MaCRA: A model-based framework for maritime cyber-risk assessment. UoP Technical Report, 2018.
[32] 福戸淳司．自律船について．日本航海学会誌 NAVIGATION, 2016, 195: 2-3.
[33] 福戸淳司．自律船研究の動向．日本航海学会誌 NAVIGATION, 2017, 200: 4-11.
[34] 南健悟．無人船舶の航行と海上衝突予防法．海事交通研究, 2017, 66: 91-102.
[35] 梅田綾子, et al. 自律運航船の実現に向けた法的課題への対応．日本機械学会論文集, 2018, 84.860: 17-00464-17-00464.
[36] 逸見真．法の存在する意義-自動化船，自律化船と法．日本航海学会誌 NAVIGATION, 2017, 200: 28-33.
[37] 藤本昌志．自律船の出現に伴う法的問題．日本航海学会誌 NAVIGATION, 2017, 200: 24-27.
[38] 柏卓夫．自律運航実現を支える運航支援技術．日本航海学会誌 NAVIGATION, 2017, 200: 18-23.
[39] “国際海事機関” http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf（参照 2018-08-09）
[40] TUCCI, Andrew E. Cyber risks in the marine transportation system. In: Cyber-Physical Security. Springer, Cham, 2017. p. 113-131.
[41] “合衆国沿岸警備隊「Cyber Strategy」” https://www.overview.uscg.mil/Portals/6/Documents/PDF/CG_Cyber_Strategy.pdf（参照 2018-08-09）
[42] “ENISA”https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/dependencies-of-maritime-transport-to-icts（参照 2018-08-09）
[43] “内閣サイバーセキュリティセンター 「重要インフラの情報セキュリティ対策に係る第４次行動計画」” https://www.nisc.go.jp/active/infra/outline.html（参照 2018-08-09）
[44] “国土交通省「物流分野における情報セキュリティ確保に係る安全ガイドライン 第３版（平成 28 年 4 月 1 日改訂）” http://www.mlit.go.jp/common/001127564.pdf（参照 2018-08-10）
[45] “国土交通省「海事生産性革命（i-Shipping）の全体像」” http://www.mlit.go.jp/common/001150897.pdf（参照 2018-08-09）
[46] “（一財）日本船舶技術研究協会「活動紹介」 https://www.jstra.jp/html/a03/a3b02/post-25.html（参照 2018-08-09）
[47] “日本経済新聞「船舶 IoT の共通基盤 2022 年に 550 隻のデータ活用へ」（2018 年 6 月 1 日）” https://www.nikkei.com/article/DGXMZO31246200R00C18A6000000/（参照 2018-08-09）
[48] “University of Plymouth Maritime Cyber Threats research group”https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group（参照 2018-08-10）
[49] 島田裕樹．海事インフラのサイバーセキュリティ．情報セキュリティ大学院大学，2017.
[50] JONES, Kevin D.; TAM, Kimberly; PAPADAKI, Maria. Threats and impacts in maritime cyber security. 2016.
[51] HAYES, Christopher R. Maritime cybersecurity: the future of national security. 2016. PhD Thesis. Monterey, California: Naval Postgraduate School.
[52] “Marsh LLC The Risk of Cyber-Attack to the Maritime Sector” https://www.ahcusa.org/uploads/2/1/9/8/21985670/the_risk_of_cyber-attack_to_the_maritime_sector-07-2014.pdf（参照 2018-08-10）