Vol.2019-DPS-178 No.2
Vol.2019-CSEC-84 No.2
2019/3/4

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，重要インフラ，

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

1.1 研究の背景

近年，わが国政府は海事産業の振興と国際競争力向上のため，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 年までに自動運航船の実用化も目指しているところであり，これら技術にサイバーセキュリティの確保は重要な産業である．また，安全保障の観点からも，海運・造船を含む海事産業は重要な産業である．さらに，現在サイバー空間の安全保障を取り巻く環境は厳しさを増す中，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，特にわが国については，現状整理と課題抽出の段階にあると言えよう．

1.2 本研究の目的

本研究の目的は，わ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である．すなわち，本研究ではわが国を中心に据えながら海事サイバーセキュリティを可能な限り俯瞰し，その概要を把握するため，海事産業の情勢，船舶の基礎的な情報，関連研究，わが国と諸外国の海事サイバーセキュリティ関連情勢，取り組み等網羅的に取り上げることで，現在論じられている主要なトピックを整理し，検討が必要な課題を洗い出す．また，現時点で想定できるサイバーセキュリティの不備に起因する船舶事故について，どのようなケースが想定できるのか例示する．

1.3 本研究の貢献

本研究の貢献は，わが国で未だ研究が活発とは言い難い状況にある海事サイバーセキュリティの現状についてサーベイを行い，この分野の現状と課題についてまとめることにより，海事サイバーセキュリティに関連する課題について広く認知を得て，関心を集めることで，本研究領域の発展の基礎となることにある．

1.4 本稿の構成

2. 日本の海事関連情勢

2.1 重要インフラとしての海事

日本は四方を海に囲まれた島国であり，国土面積約 38

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

Vol.2019-DPS-178 No.2
Vol.2019-CSEC-84 No.2
2019/3/4

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a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]．これは世界第 6 位の広さである．

この島国で我々が日々の生活を送るために必要な石油，石炭，ガスなどエネルギー，その他資源，工業原材料，食糧等は多くを輸入により賄っている．これら物資の輸入はその 90%以上を船舶による海上輸送で行われている．わが国の 2017 年の国際航空貨物輸送量約 175 万トン2に対して海上貨物輸送量は約 9 億 3,300 万トン[3]に達していることからもわが国の輸出入貨物輸送は海路に大きく依存していると言える．また，国内貨物輸送の約 40%[4]を内航海運が担っており，その海上輸送の手段として用いられているのが船舶である．

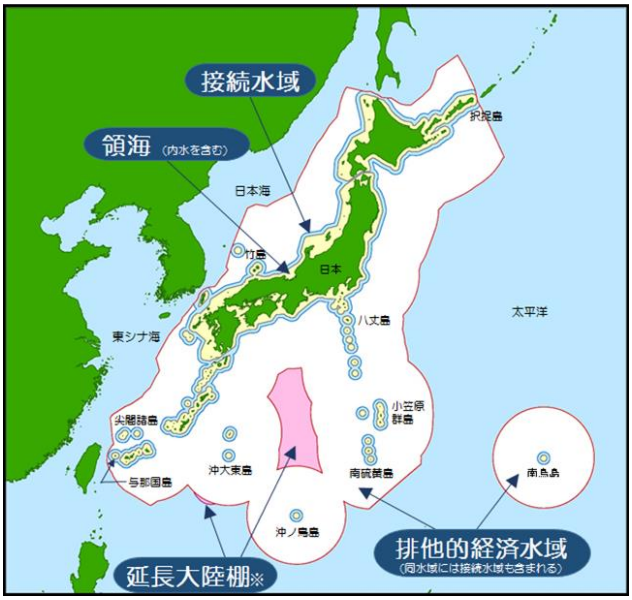

図 1　日本の管轄海域[1]

この船舶を中心に造船業，海運業，港湾等多くの産業により構成されているのが海事産業である．海事産業は日本の海上輸送を支えている存在である．造船業を例に挙げると，小規模事業者から大規模企業に至るまで，約 1,100 の事業所が約 8 万人の従業員を雇用し，生産高は約 2 兆円規模 3 である．

海上輸送が我々の日々の生活を支えているところ，これがもし安全に行われなくなり，停止してしまった場合，どのような影響があるだろうか．エネルギー，原材料の不足による製造業を初めとする企業の操業停止等経済的な混乱，物資の不足による国民生活の混乱，長期化すればわが国の存立も脅かされる事態も懸念される．つまり，海上輸送やそれを支える海事産業はわが国の重要なインフラと言える．内閣府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」[5]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なっている．

2.2 海事産業とサイバーセキュリティ

海事産業とサイバーセキュリティがどのように関係するのかを理解するため，海事産業分野で導入の進むデジタライゼーションについて述べる．

海事産業とは，海運業，造船業を中心としてそれに関連する多くの産業が集まりクラスターを形成している．その関連度合いが特に高いものを中核的海事産業と呼び，そこには海運業，造船業，船会社などが含まれ，隣接する産業等を含め海事クラスターを形成している．海事クラスターには港湾，倉庫・物流，商社，損害保険，漁業，水産業等多くの産業が含まれる．

近年，この海事産業を取り巻く環境に変化が生じている，現在海事産業は，外国企業に対し国際競争力の低下，労働者人口の減少等課題を抱えている．わが国政府はこの状況を改善するために海事産業への ICT 導入を推進している．国土交通省は 2016 年を「生産性革命元年」，2018 年を「深化の年」に位置付け[3]，造船所での IoT 導入，船舶運航の自動化等先進技術を取り入れることで生産性，効率性を向上させ，海事産業の国際競争力アップを目指している．

また，内閣府の発表した未来投資戦略 2018[6]では 2025 年までに自動運航船の実用化を目指すとの記載もあり，海事産業の IT 化（「デジタライゼーションの推進」とも言われる）が今後一層進むことが予想される．

図 2　海事クラスターの構成（一部抜粋）

本稿では船舶におけるサイバーセキュリティを中心に海事サイバーセキュリティを論じる．

a 管轄海域とは国連海洋法条約に従い沿岸国に出入国管理等の規制や，資源開発等の権利を認められている海域

Vol.2019-DPS-178 No.2
Vol.2019-CSEC-84 No.2
2019/3/4

近年船舶の IT 化が進んでおり，船舶の運航にコンピュータシステムが欠かさないものとなっている．また，衛星通信技術の進歩により大容量通信も可能となり，ネットワークと常時接続する船も現れている．先述の通り，政府の施策として海事産業のデジタライゼーションが進み，今後「コネクテッド」な船舶が増加することが予想され，それに伴い陸上と同様なネットワーク環境になっていくため，サイバーセキュリスクについても陸上と同様に厳しいものになっていくであろう．

2.3 船舶の特徴

ここでは，海上輸送に欠かすことのできない船舶について述べる．

船舶とは一般的に水に浮かび，水の上を航行するために用いられる構造物をいう．法的にはそれぞれの法律で定義が多少異なるが，一般的には水上を航行する構造物を指す．

船舶の特徴としては以下のものが挙げられる．

- 水上を航行する
- 小型のものから巨大なものまで存在する
- 大量輸送が可能
- ライフサイクルが長い
- 航行中は孤立
- 移動可能なプラントとしての側面を持つ
- サプライチェーンが長い

2.4 船舶の種類とリスク

2.4.1 タンカー

タンカーは原油，液化天然ガス，液化プロパンガス，化学薬品等可燃性，有害性のある液体を輸送するため，万一積荷が漏れ出た場合は火災，環境汚染などを引き起こす可能性がある．また，わが国は原油のほぼ 100%を海外からの輸入に依存しており，原油タンカーはわが国のエネルギー安定供給に欠かすことのできない存在である．

2.4.2 客船，フェリー

近年，わが国でも寄港の増えているクルーズフェリーや，国内航路を定期運航するフェリーなど旅客を運ぶ船では，事故が発生すれば多くの人命に危険が及ぶことになる．

2.4.3 コンテナ船

コンテナ船は物流の中核を成している貨物船であり，我々の生活を支える様々な物を運んできてくれる．コンテナ船の運航が阻害されれば，我々の日常生活に必要な物資の供給に影響が出る．

2.4.4 ばら積み貨物船（バルクキャリア）

鉄鉱石や石炭，穀物，木材，チップ，セメント，肥料，塩など，多種多様な資源を輸送する船であり，これらの船が事故を起こせば我々の生活に必要な製品の生産，エネルギーの供給に影響が出るとともに，事故現場周辺の環境に影響を与える恐れがある．

2.4.5 自動車専用船

一般乗用車や建設機械を大量に運搬することに特化した船で，わが国の主要輸出品の一つである自動車の輸送を担っている．これの運航が滞ることがあれば，わが国の経済のみならず，自動車輸入国の経済活動にも影響を与え得ることとなる．

2.5 船舶の航行区域とリスク

船舶の航行している場所によってもリスクの度合いが変わってくるので，この点について本稿では東京湾のような都市部の沿岸と外洋で検討する．

2.5.1 外洋

本稿では外洋とは距岸（陸地からの距離）概ね 24 海里b以遠の海域を外洋と定義して述べる．

外洋は航行する船舶間の距離も大きく，人の居住する陸地からも遠いため，船舶事故発生時の付近への影響は湾外，沿岸部に比較すると限定的である．また，事故の内容によるものの，被害制御等の対応に時間的余裕も見込める．しかし，外洋を航行する船舶は事故発生時の陸上からの支援が困難であり，洋上でのサイバーインシデント対応時，陸上のようにセキュリティエンジニアのオンサイトでの対応が困難である．

2.5.2 湾内，沿岸域

本稿では湾内，沿岸域の定義を概ね 24 海里未満の海域，特に陸地に近いところについて述べる．

東京湾，伊勢湾，大阪湾のような大都市圏沿岸や瀬戸内海のような人口の多い地域や，沿岸で漁業をしている海域での船舶事故は人命，環境に与えるリスクが高く，直ちに国民生活へ影響を与える恐れがある．原油タンカーによる原油流出事故，海上に架けられた橋に船舶が衝突，接触したことによる事故等船舶事故が国民生活や環境に影響を与えた事例は複数存在し，今後これらの事故の原因として「サイバー」が新たに加わる事態に備える必要がある．

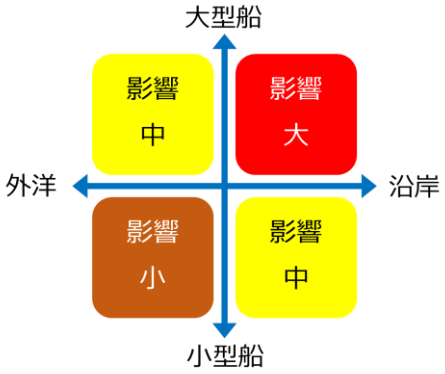

図 3　船舶の大きさ，航行区域による船舶事故影響の比較

b1 海里=1,852m，24 海里=約 44.5km

2.6 船舶搭載システムとサイバーセキュリティ

船舶のサイバーセキュリティについては搭載されているシステムについて，サイバーセキュリティ上のリスクが指摘されている．ここでは IMO や海事関連機関のガイドラインを参考に主なシステムを分類して述べる．

2.6.1 通信システム

船舶の通信に用いられるシステムで，近年は衛星通信の通信速度が速くなったことで，常時インターネット接続される船舶も存在する．

2.6.1.1. 超小型衛星地球局（VSAT）

VSAT（Very Small Aperture Terminal）は通信衛星用の超小型地球局である．船舶ではこれのおかげで航海中も常時インターネット接続が可能になりつつある．そのため，船内の IT システムや制御システムも VSAT を通じで外部ネットワークと接続されるようになってきている．

例えば，舶用機器の稼働状況を陸上でモニターし，機器の故障予測や予防保守といった機器のメンテナンスの効率化に役立ったりしている．

その VSAT についても脆弱性が指摘されている．BOTHUR(2017)[7]らは複数の VSAT をテストしたところ，すべてのデバイスはプロトコルと実装において脆弱であると結論付けた．それらは認証，暗号化，または完全性チェックなしでデータを平文で送信するため，攻撃者が偽の信号や悪質なコードを挿入して，デバイスをシャットダウンしたりシステムを破損させたりできる可能性があると指摘している．つまりこれらの脆弱性がある機器が分かっていれば，SHODANcを用いて検索することができるため，脆弱性のある VSAT を使用している場合，航行中の船舶に陸上から攻撃できる可能性があることを示している．この問題についてはイギリスのサイバーセキュリティ企業ら[8][9]も指摘 しており，衛星による常時接続は船舶をハッキングの危険にさらしていると述べている．

船舶における常時接続サービスは，通信料金の定額制の導入により船員の福利厚生目的でも利用が広がりつつあるため，その動向に注意する必要がある．

2.6.2 ブリッジシステム

航海計器とも呼ばれる船舶の運航に用いられるシステムを指す．

2.6.2.1. 衛星測位システム（GNSS : Global Navigation Satellite System）（GPS : Global Positioning System）

民間の全地球測位システム（GPS）は，政府および民間産業の両方で広く使用されている．これらには警察，消防など公共サービス，物流，公共交通，農業機械，自家用車，宇宙船，海上輸送，航空輸送もナビゲーションに GPS システムを使用している．Warner（2003）[10]らによれば，軍用 GPS 信号だけが暗号化（認証）されているものの，民生用 GPS は暗号化されていないため安全でなく，GPS 衛星からの信号も弱く，地球の表面で測定された GPS 信号強度は約-160dBw（$1x10^{-16}$ ワット）で，これは 10,000 マイルの距離から 25 ワットの電球を見るようなものと例えている．そのため電波を遮蔽，もしくはより強度の強い電波をかぶせることで簡単に妨害することができる．しかし，Warner らは電波の妨害について，GPS 受信機は位置および時間を決定するのに必要な GPS 信号が途切れれば，知ることができるためさほど問題ではなく，GPS 受信機に偽の GPS 信号を送る「なりすまし」の方が悪質であると指摘している．

GPS の懸念については，測位システムを GPS のみに依存するのではなく，Galileodのような他の測位システムも利用できるようにバックアップの確保も重要だろう．米海軍では，一度廃止されていた天文航法の教育を再開[11]しているところからもバックアップ手段の重要性がうかがえる．

2.6.2.2. 電子海図情報表示装置（ECDIS）

ECDIS（Electronic Chart Display Information System）はディスプレイ上に電子海図のほか航海に必要な種々の情報を表示する航海計器である．

図 4　ECDIS の表示例e

国際航海に従事する総トン数 500 トン以上の旅客船と総トン数 3,000 トン以上の貨物船には ECDIS の搭載が義務化されている．

オートパイロットf（自動操舵装置）と接続することで電子海図上に設定した航路を自動で航行することも可能である．

BOTHUR(2017)[7]らは ECDIS ソフトウェアの実装には，さまざまな弱点があると指摘している．多くの場合，システムはセキュリティ更新プログラムが適用されていない従来のコンピューター（Windows XP デスクトップなど）で実行され，地図データの更新gは，インターネットを介して，

c https://www.shodan.io/

d https://www.gsa.europa.eu/

e https://www.furuno.com/img/prev/jp/markets/merchant/ecdis/FMD-3200_3300/userinterface_img_016_l.jpg

f ここでいう自動操舵とは障害物を避けながら自律的に航行するのではなく，あらかじめ設定してあるコースをたどる機能を指す．

g 海図は陸上の地図より頻繁に改正が行われる．水深の変更や航路の障害

またはデータをダウンロードした後手動で USB または DVD を介して行われる. また, レーダー, AIS, GPS, VSAT, ICS 等と接続されているため, 攻撃面が大きいとし, ECDIS に改ざんされたデータが送られたとき, 最悪の場合衝突や, 乗揚げの危険性があるとしている.

2.6.2.3. 船舶自動識別装置（AIS）

船舶自動識別装置（Automatic Identification Systematism) とは船舶の効率的な運航の支援，航行安全，環境保全，船舶交通業務運用の改善のために用いられるシステムである.

AIS は VHF 帯無線により, 船舶間または船陸間で情報の送受信を行う．その内容は船舶の船名，コールサイン，線種等の静的情報，船位，進路，速力等の動的情報，目的地，到着予定時刻等の航海情報である．それら情報を相互に参照することで船舶交通の円滑化や安全に活用している．また，AIS にはメッセージを任意の相手または不特定の相手にブロードキャストすることもでき，沿岸の海上保安当局が航行上の安全情報を提供するために用いている．また，電子海図上に仮想航路標識（電子海図上にのみ表示されるマーク）を表示する取り組みhも始まっている．これは設置場所の水深が深い等の理由で実際に航路標識の設置が困難な場所において，電子海図上に航路標識を表示させることで船舶交通の安全に活用するものである.

図 5　AIS によるバーチャル航路標識の例i（出典元画像を一部編集して引用）赤枠内のマークが矢印の指す位置に表示される

AIS はジャミングやなりすましの脆弱性があると指摘されている．BALDUZZI(2014)ら[12][13][14]は AIS が使用するプロトコルに存在する認証の欠如，時刻確認，整合性確認の欠如を指摘している.

このような問題がある上，AIS に対する攻撃は約 2 万円程度で購入可能な VHF 無線機を利用することで可能であると述べている．これらの攻撃の防御策は AIS メッセージの暗号化や認証をすることだが，すべての AIS 受信機を更新するのは難しいため，対策は容易でない.

東京湾のような船舶交通の激しい海域でこのような攻撃がされると容易に交通の混乱を引き起こす可能性がある.

船舶搭載システムとしてはこのほかに船内で基幹業務システムとして用いられている IT ネットワーク, 船内でエンジン，発電機，ポンプ等機器類の制御に用いられる産業制御システム（ICS）があり，これらについても BOTHUR(2017)[7]らセキュリティ上のリスクを指摘している.

2.7 自動運航船の研究・開発状況

自動運航船はわが国でも 2025 年の実用化を目指して研究開発が進められているところである．また海外でも欧州で盛んに開発が進められており 15，2018 年 12 月に Rolls-Royce とフィンランドの国営フェリー運航会社 Finferries が最初の完全自律型フェリーの試験運行に成功したと報じられている．[16]

自動運航船に必要なサイバーセキュリティについて，KATSIKAS（2017）[17]は自律型船のサイバーセキュリティを確保するための包括的なアプローチを採用する必要があると主張している．KATSIKAS は船内の複雑なシステムがセキュリティを考慮されていないインターネットに接続することによるリスクを懸念しており，それがサイバーセキュリティ対策を複雑にしていると指摘している. そのため，新しいシステムが設計段階からセキュリティ（およびプライバシー）を念頭に置いて構築されていない限り，サイバーセキュリティの問題に直面するだろうと述べている.

2.8 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検討する．まず挙げられるのはインフラが船舶（海上）と陸上に分かれていること．そのため，航海中の船舶へ物理的にアクセスすることが困難であるため，セキュリティインシデントが発生した際に陸上のようにセキュリティベンダーのエンジニアが駆けつけてオンサイト対応するということができない. そのため，ある程度乗員で対応できるようにする必要があるではないだろうか.

次に現在船舶に搭載されている機器類にはセキュリティを考慮した仕様になっていないものが使用されており，それらが IT ネットワークと接続され，VSAT を介しインターネットとつながるようになってきたことも挙げられる.

航海中孤立することについて，航空機も陸上と空に分かれ，飛行中は孤立するものの，飛行時間は船舶に比較して短いため，その点では海事分野の方が特徴的と言えよう.

海事分野はサイバーセキュリティに対する取り組みが他産業より後発であることも海事分野のサイバーセキュリティが発展途上であると言える.

3. 国内外の海事サイバーセキュリティに対す

物などの情報もあるため海図を最新に保つことは航海の安全上重要である.
h “海上保安庁「わが国初！バーチャルＡＩＳ航路標識の運用開始について」” https://www6.kaiho.mlit.go.jp/05kanku/info/ais.html
i http://www6.kaiho.mlit.go.jp/05kanku/info/akashikaikyo.jpg

る取り組み

3.1 諸外国の状況

国際海事機関（IMO）j，各国船級k協会では主にマネジメントベースのサイバーセキュリティガイドラインを策定している．これらガイドラインは ISO27001，NIST サイバーセキュリティフレームワークを参考に策定されている．

3.2 わが国の状況

わが国では国土交通省では第 3 期海洋基本計画18で示されている通り，海事産業の振興，国際競争力向上のため，平成28年1月に交通政策審議会海事分科会に海事イノベーション部会を設置l，船舶の開発・設計，建造から運航に至る全てのフェーズで生産性向上を目指す「i-Shipping」と海洋開発分野において海洋開発市場の成長をわが国海事産業が獲得することを目指す「j-Ocean」からなる「海事産業の生産性革命」なる政策を推進している．

このように積極的に海事産業のデジタライゼーションが政策として推進されている．しかし，これらの政策の中にサイバーセキュリティについての記載はほとんど見られないのが現状である．

4. 想定される海事サイバー攻撃例

ここでは，現状どのような海事サイバー脅威によりどのような結果が生じ得るか，またどのような問題がこのような結果を生じさせ得るのかを述べる．以下のシナリオはあくまでも将来発生するかもしれない事例を述べているものであり，サイバーセキュリティ体制についてあまりにもずさんではないかとの指摘もあるかと思われるが，便宜上そのような設定にしていることと，実際に発生した事案ではないことを断っておく．

- **シナリオ：旅客船の船内システムへの攻撃**
  - 2020 年 7 月某日午前 8 時頃，東京オリンピックに合わせ東京都江東区に新設された東京国際クルーズターミナルに入港予定のクルーズ客船「X」（総トン数 150,000 トン，長さ 350m，乗客 4,300 名，乗員 2,000 名乗船）は東京湾横須賀沖の浦賀水道航路 を東京向け速力 12 ノット で北上中のところ，突如発電機が停止．通常であれば非常用発電機へ切り替わるところ切り替えができないまま船内電源を喪失（ブラックアウト），操船不能に陥ったため，やむを得ず航路内で投錨 した．その結果航路内で立ち往生する形になり，浦賀水道航路は航路航行義務のあるされた．そのため貨物船，タンカー等他の入港船が入港できなくなり，一時東京湾内はパニックとなった．客船「X」の船舶代理店が手配したタグボートにより同日 17 時東京国際クルーズターミナルに着岸した．
  - その間コンテナ船やタンカー等の入出港が遅れたため，物流への大きなダメージを与えることになった．
  - 海難調査のため，海上保安官，運輸安全委員会 の船舶事故調査官が臨場して，調査を開始した．
  - 原因を調査したところ，発電機を制御するシステムがシャットダウンしていることが判明．さらに船内の PC が，マルウェアに感染していたことがわかった．船舶運航会社はセキュリティ企業に依頼し詳細な調査を実施するも，調査に必要なログが保存できていなかったため調査は困難を極めた．
  - その後の調査の結果，マルウェア感染した PC（客船「X」機関科乗組員 使用）から発電機制御システムに意図しないアクセスが発生していたことが判明した．PC の使用者である機関科乗組員に事情を聴いたところ，ブラックアウト発生の数時間前に船内で USB メモリ（その船で使用している発電機メーカーのロゴがプリントされていた）を拾っており，ブラックアウト発生の数分前に PC に接続してメモリ内のデータを確認したところデータは何も保存されていないように見えたことから USB メモリを取り外し，機関室で入港準備作業をしていたところブラックアウトが発生したとのことであった．同様の USB メモリがその後船内で複数発見されたが，それらが他の PC に接続されることはなかった．サイバーセキュリティ企業の解析の結果，USB メモリにはこの客船の発電機制御システムをシャットダウンさせ，以後起動できないようにすることを狙ったマルウェアが保存されていることが判明した．また，客船「X」PC で使用しているアンチウイルスソフトでは検知のできないマルウェアであった．
  - 海上保安庁は本件を何者かがマルウェアを用い客船「X」発電制御システムを停止させ，ブラックアウトを招いたとして，不正指令電磁的記録作成等違反 被疑事件として捜査を開始したものの，海上保安庁は同種事件捜査の経験がないため，警察の支援を得ながら行うこととなった．
  - 後に日本の捕鯨政策に反対する海外のグルー

j IMO:海上の安全，船舶からの海洋汚染防止等，海事分野の諸問題についての政府間の協力を推進するために1958年に設立された国連の専門機関である．

k 船級 とは，海上保険業者，荷主などの利便のため，船級協会が付与する船舶の格付け．船級協会は，船体，艤装(ぎそう)，機関について検査し，協会の規格に該当すると認めた船舶に対して与えるものである

l http://www.mlit.go.jp/maritime/maritime_tk5_000039.html

プがウェブサイト上で犯行声明を出し，日本周辺海域で再開された商業捕鯨に抗議すると訴え，捕鯨を中止しない限り同種の攻撃を継続すると訴えた．

- 海上保安庁は船舶に対するサイバー攻撃が実際に発生したことを受けて，サイバー犯罪捜査体制構築を緊急の課題として取り組むこととなった．運輸安全委員会も事故原因の解明にはサイバーセキュリティに関する知識が必要だとし，事故調査官に求められる能力の見直しを迫られることとなった．わが国にとって海上輸送の安全確保をするためのサイバーセキュリティの重要性を再認識する教訓となる事件であった．
- 海運を初めとする海事産業にも国内で実際にサイバー攻撃に起因する事故が発生したことから，各社がサイバーセキュリティに真剣に取り組む契機となる事件となった．
- 本シナリオで示すサイバーセキュリティ対策の問題点については
  - ✧ 攻撃者：ハクティビスト
  - ✧ 動機：自己主張
  - ✧ ターゲット：客船の発電制御システム
  - ✧ 手法：USB（発電機メーカーのロゴがプリントされた物）に仕込んだマルウェアに感染させるもの
- であり，今回乗組員が不用意に出所不明の USB を PC に接続してしまったことが直接の原因である．攻撃者は USB に発電機メーカーのロゴをプリントして，成功確率を高める工作をしており，乗組員の警戒心を下げることに成功している．
- かかる場合，船内でサイバーセキュリティについて通常実施するべきマニュアル等を整備し，出所不明のデバイスを業務システムに接続しないといった運用を乗組員に実施させるといったことが必要だが，これができていなかった．
- また，原因調査で必要となるデジタルフォレンジックに必要なログが保存できていないことも原因の特定を遅らせる結果となっている．また，今回はバックアップである非常用発電機への切り替えもできなかった ため電源の復旧ができなかったため，航路を閉塞する時間が長くなったことも被害の拡大要因となっている．
- 陸上の組織で一般的に行われているであろうサイバーセキュリティ対策が船内でも実施できていれば，防げたであろう．それができていない場合，船舶においてはこのような結果を生じさせる危険があることを示したシナリオである．
- 派生する問題点として，事故の調査，捜査をする上での調査官，捜査官の能力，組織の問題も露呈するケースとなった．最終的には，客船が航行不能になり航路で立ち往生した結果，航路を閉塞し，東京湾の海上交通に大規模な影響を与えたわけだが，その原因がサイバー攻撃によるものであり，海上保安庁も運輸安全委員会も経験のない事件・事故となったため，捜査，調査に支障をきたす可能性があることを示した．これは早急に検討の必要な課題であろう．

5. 考察

これまで海事サイバーセキュリティの現状について述べてきた．諸外国の状況，海事関連機関の動向を見る限り，海事分野に潜在的なサイバーリスクがあり，船舶の安全運航上の問題が生じる危険があることを指摘している．そのため IMO，各船級協会，各国監督官庁等はこれまでの船舶安全対策にサイバーセキュリティも加えるようになってきた．現在発表されている各ガイドラインを見ると，基本的には NIST のサイバーセキュリティフレームワークを参考に作成されており，リスクの特定，脆弱性の特定，リスク評価，保護，検知手段の策定，インシデントへの対応といった手順が記載されている．IMO ガイドラインでは具体的に示されていない評価手法について，DNV-GL ガイドラインでは Bow-Tie Method の利用を推奨するといったように，ガイドラインを実行する上で具体的手法を示すものもあり，ガイドラインによりその位置づけは若干異なるため，各ガイドラインの目的等をよく把握して活用する必要があるだろう．わが国ではどのようなガイドラインが作成されるか今後の国内動向を継続して調査したい．

学術分野では主に海外で海事サイバーセキュリティを対象とした研究が行われており，専門の研究グループ を持つ大学も存在する．また，海事サイバーセキュリティのシンポジウム も実施されていることからも注目されていることが伺える．先行研究では海軍，沿岸警備隊の著者も見受けられ，安全保障の面からも研究対象となっている．わが国でも，IMO，海外船級協会の取り組みを受け，JSTRA が調査研究を実施中であるが，海外のような活発さは見られず，大学等の研究機関での研究はほとんど見られない．現状わが国では海事関連団体での調査研究が始まって日の浅い状況と言えるだろう．

国内で学術分野での研究者がほとんど見られないのはなぜだろうか．海事サイバーセキュリティが海事というある種特殊な分野でのサイバーセキュリティであり，これまではサイバーセキュリティと関係しない分野であったためだと考えられる．そのため，今後は海事サイバーセキュリティについて広く認知されるよう，継続した研究の発表が必要である．また，今後は既存の海事関連研究者とサイバー

セキュリティ研究者が情報交換や双方の知見が活用できる場が求められる．そのため，海事サイバーセキュリティをテーマとしたシンポジウムやカンファレンス等，分野を横断した研究者の発表，交流を促進するような施策を政府が進める海事産業のデジタライゼーション関連施策に加えるといった検討も必要だろう．

わが国政府も海事産業のデジタライゼーション推進施策を実施中で，積極的な技術開発支援をするものの，サイバーセキュリティをテーマとするプロジェクトは見られず，自動運航船に関する部分でセキュリティに触れられているのみである．

そもそも海事サイバーセキュリティを所管する官庁がはっきりしていない．内閣府の定める 14 の重要インフラに海運を含む物流分野が入っているものの，海事産業のうち物流に含まれない産業，例えば造船業は重要インフラに含まれていない．そもそも船舶に関する種々の規制，監督を所掌するのは国土交通省であるが，未だ海事分野のサイバーセキュリティをどの官庁がどのように監督するのかもはっきりしない．また，現在船舶事故が発生した場合は海上保安庁が調査・捜査することになるが，仮にサイバー攻撃に起因する船舶事故が発生した場合，海上保安庁には警察の様なサイバー犯罪専門の捜査官はないため，対応を検討する必要がある等，政府として海事サイバーセキュリティに今後どのように取り組んでいくのか検討が急がれる．そもそも陸上の攻撃者が船舶のシステムに不正アクセスを行った場合の捜査管轄等が法的，制度的に検討が必要な事項は少なくないだろう．

重要インフラ防護においても警察と重要インフラ事業者の連携が始まっている．海事分野については海上保安庁も同様の取り組みを始める必要があるだろう．現在重要インフラ防護のためのサイバーセキュリティに関する調査検討のため平成 27 年 2 月，内閣に重要インフラ専門調査会 がおかれている．以来，17 回 にわたり会合が開かれている．これらの会合に重要インフラ事業者を所管する官庁幹部もオブザーバー参加しているところ，海上保安庁の参加はない．物流は国土交通省が所管しているところではあるが，海上の安全確保を担う海上保安庁も参加することで，重要インフラ事業者や他官庁と情報共有，意見交換が行え，さらなる重要インフラ防護対策に資することができるのではないだろうか．

特に海上におけるサイバーリスクに起因する事故，犯罪は既にいつ起きるとも分からないため，海上保安庁はこの問題を喫緊の課題として取り組む必要があろう．

海上保安庁のサイバーセキュリティについての所掌事務は自組織の情報通信システムの安全確保とされている．また，船舶事故調査，犯罪捜査（不正アクセス禁止法等のサイバー犯罪を除く）に必要な航海計器のデータ抽出や PC，スマートフォンのデジタルフォレンジックは行っているものの，今後船舶に対するサイバー犯罪が発生した場合に現状では円滑な対応は困難であると考えられる．

海事サイバーセキュリティにおいては一般的なサイバーセキュリティに関する知識に加え船舶システムに関する知識も必要となり，サイバーリスクに起因する事件，事故対応にあたる海上保安官にはこれらの能力が求められ，人材の確保，育成，組織体制の構築が急がれる．

6. おわりに、今後の展望

ここまで，海事サイバーセキュリティについて可能な限りその全体像がつかめるような論文を目指してきたが，紙面の都合上，ここで触れることができたのは一部である．今後は海事サイバーセキュリティを向上するためにどのような政策が必要か等，制度的なものも研究テーマとしたい．また，海事サイバーセキュリティはまだまだ新しい分野であり，新たなトピックも日々でてきている状況である．国内での研究者もほとんど見られないため，今後も研究を続けていく所存である．

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 2018-12-09）
2 “国土交通省 「航空輸送統計調査 年報 平成 29 年分」” http://www.mlit.go.jp/k-toukei/search/excel/11/11201700a00006.xlsx（参照 2018-12-20）
3 “国土交通省海事局 「海事レポート 2018」” http://www.mlit.go.jp/maritime/maritime_tk1_000072.html（参照 2018-12-20）
4 “日本船主協会 「SHIPPING NOW 2018-2019」” https://www.kaijipr.or.jp/shipping_now/pdf/allpage2018.pdf（参照 2018-12-20）
5 “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」” http://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf（参照 2018-12-20）
6 “内閣 「未来投資戦略 2018」” https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_zentai.pdf（参照 2018-12-20）
7 BOTHUR, Dennis; ZHENG, Guanglou; VALLI, Craig. A critical analysis of security vulnerabilities and countermeasures in a smart ship system. 2017.
8 https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships/（参照 2018-12-10）
9 “IOActive A Wake-up Call for SATCOM Security” https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf（参照 2018-12-12）
10 WARNER, Jon S.; JOHNSTON, Roger G. GPS spoofing countermeasures. Homeland Security Journal, 2003, 25.2: 19-27.
11 “Washington Post Cybersecurity fears are making U.S. sailors learn to navigate by the stars again” https://www.washingtonpost.com/news/the-switch/wp/2015/10/14/cybersecurity-fears-are-making-u-s-sailors-learn-to-navigate-by-the-stars-again/?utm_term=.a6b37e02d6d1
12 BALDUZZI, Marco; PASTA, Alessandro; WILHOIT, Kyle. A security evaluation of AIS automated identification system. In: Proceedings of the 30th annual computer security applications conference. ACM, 2014. p. 436-445.
13 “Trend Micro「A security evaluation of AIS automated identification system」” http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/

white-papers/wp-a-security-evaluation-of-ais.pdf
14 https://blog.trendmicro.co.jp/archives/8292（参照 2018-12-20）
15 “国土交通省資料” http://www.mlit.go.jp/common/001215815.pdf（参照 2018-12-20）
16 https://www.maritimejournal.com/news101/onboard-systems/monitoring-and-control/first-100-autonomous-ferry-sails（参照 2018-12-20）
17 KATSIKAS, Sokratis K. Cyber Security of the Autonomous Ship. In: Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security. ACM, 2017. p. 55-56.
18 “内閣 「海洋基本計画」” https://www8.cao.go.jp/ocean/policies/plan/plan03/pdf/plan03.pdf（参照 2018-12-10）