

海事におけるサイバー セキュリティ対策への 取り組み


東京大学大学院新領域創成科学研究科 准教授 稗方 和夫

(一般財団法人 日本船舶技術研究協会 海事分野におけるサイ
バーセキュリティ対策に関する調査研究 PM)



目次

- ▶ 海事業界について
- ▶ 船舶のサイバーセキュリティに関する動向
 - ▶ IMO
 - ▶ BIMCO
 - ▶ 各船級協会におけるサイバーセキュリティ
 - ▶ NIST Framework/800シリーズ
- ▶ 日本における取組み
 - ▶ 海事におけるサイバーセキュリティプロジェクト
 - ▶ SMS マニュアルへの指針作成
 - ▶ 海外動向調査



海事業界について



海事業界について

- ▶ 造船業や海運業など、海に携わる産業全般を指す
- ▶ 造船会社、海運会社、船級協会、舶用機器メーカー等



海運業について

- ▶ 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、ケミカル船などで11万隻程度
- ▶ 需要、船腹数は毎年3%伸びている
- ▶ 日本は世界の10%程度の船舶を運航している

海事業界の動向

- 近年、海上ブロードバンド通信の進展や ICT（情報通信技術、Information and Communication Technology）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世界的に活発化している
- 2017年4月に海上運送法を改正し、運送サービスの質を相当程度向上させることができる船舶を「先進船舶」として新たに位置づけ、先進船舶の研究開発、製造又は導入を行う事業者に対する行政手続きの特例措置等による支援を行っているところである。「先進船舶」として、LNG 燃料船等の「代替燃料船」と並んで、IoT 活用技術（インターネットに多様かつ多数の物が接続され、及びそれらの物から送信され、又はそれらの物に送信される大量の情報を活用する技術）を活用した船舶（IoT 活用船）が指定されている。

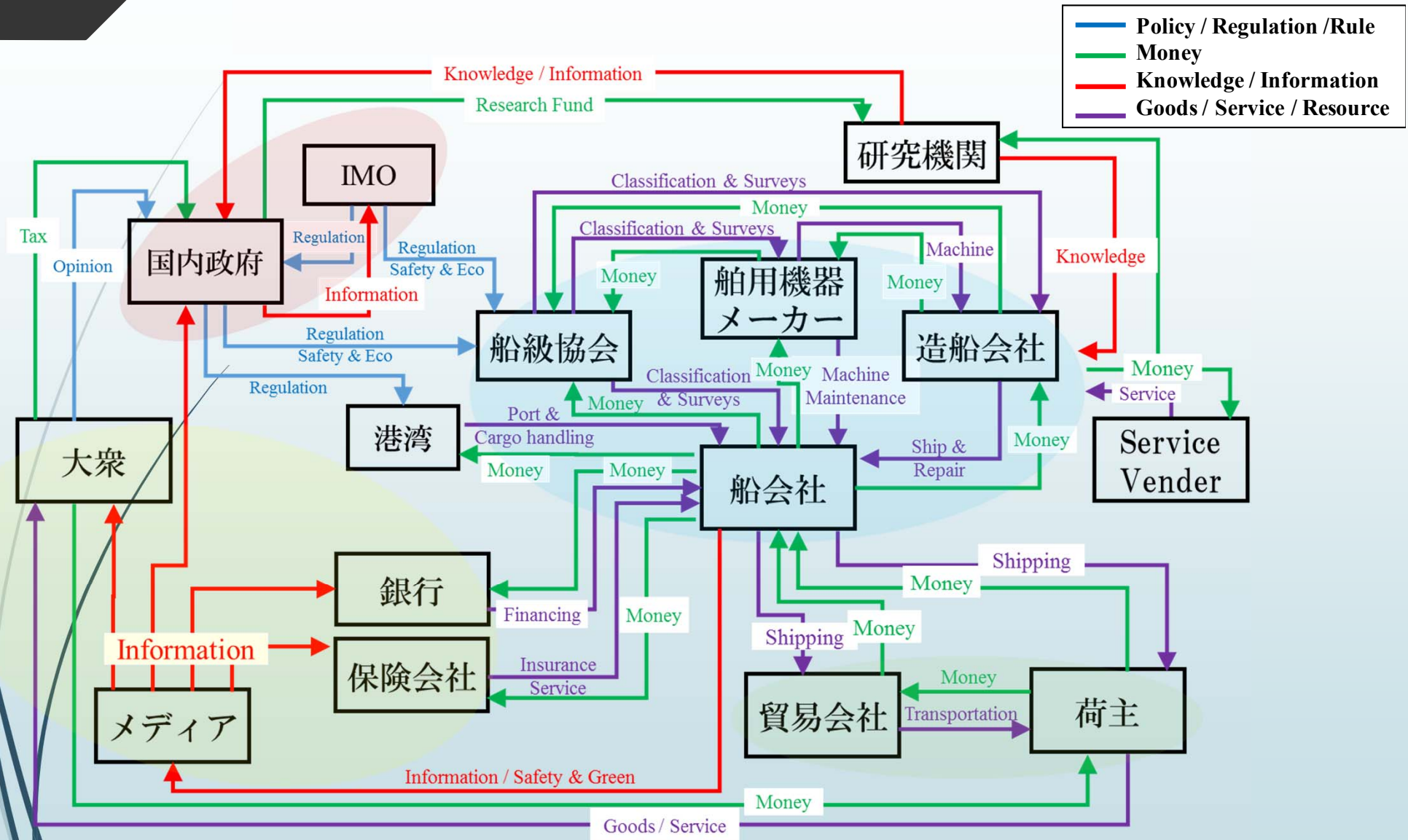
自動運航船

- 現状、自動運航船について広く共有される認識や定義はまだ固まっていないが、ここでは一般にIoT、ICT、データ解析技術等の最新技術、各種センサー及び広帯域通信により接続された陸上監視・制御拠点をを使用することで、外部状況認識（見張り）、機器等の状態監視、操船、機関制御、貨物管理・荷役、離着棧その他船舶の運航に伴う船上業務（タスク）の一部又は全部を高度に自動化（自律化）又は遠隔制御化した船舶及びその運航システムをいうものとする。

IoT活用船

- ▶ 従来、航海計器や制御機器等の船用機器は、個々が比較的独立して設置され、情報やデータ等も各機器内で閉じた形で利用されることが主であった。また、実運航時の船体・機器・機関の状態等のデータを回収して分析する環境も十分整ってはいなかった。このような中、2012年から開始された（一社）日本船用工業会と（一財）日本海事協会の共同プロジェクトである「スマートナビゲーション研究会」の場で、船内の船用機器をつなぐ通信規格が作成され、2018年、ISO規格化される見込みとなっている。また、新しい通信衛星の打ち上げ等による海上のブロードバンド通信環境も普及しつつある等、陸上と比べてやや遅れていた船舶の機器のネットワーク環境が急速に整いつつある。また、ネットワーク化が進展するのと同時に、船舶に搭載される各種機器やセンサーから得られるデータの種類や量も飛躍的に増大している。このような状況を背景に、これまでわからなかった、もしくは暗黙知、ノウハウとして蓄積されていた、実運航時の船体・機関挙動等が次第に「見える化」されるようになり、その知見は、船舶運航の効率化、高度化にすでに活用されているところである。この段階が、IoT活用船にほぼ対応する段階といえる。

海事産業に関わる利害関係




海事に関する主要な国際機関

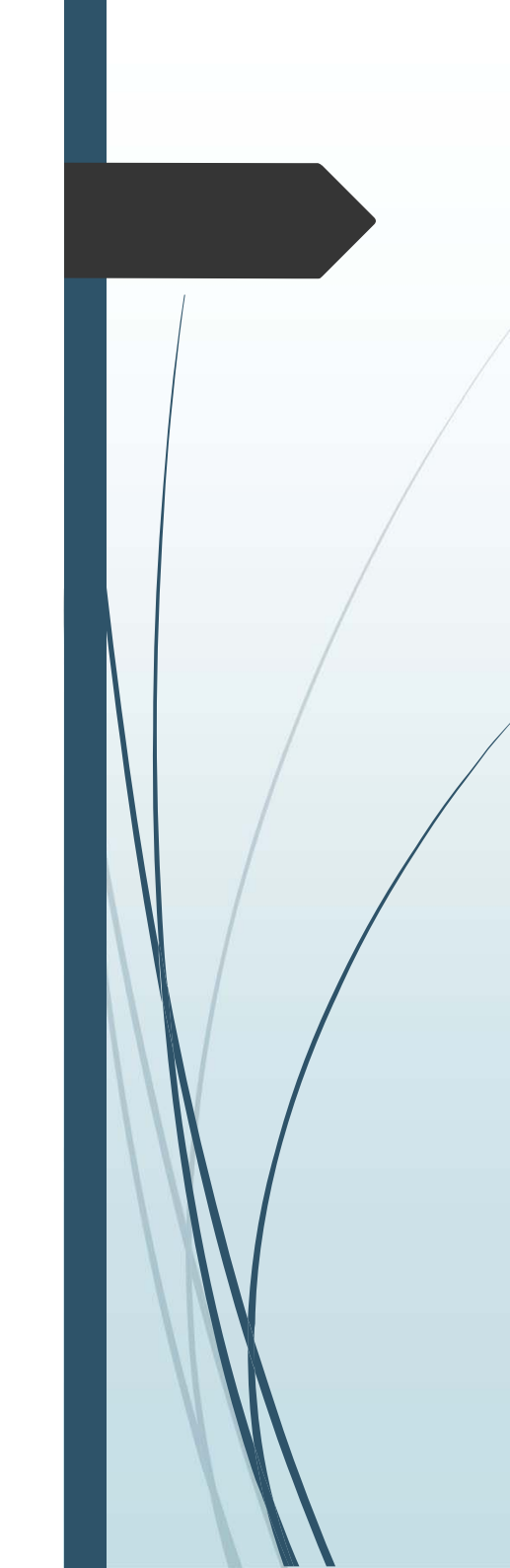
- ▶ IMO (International Maritime Organization : 国際海事機関) は、国連の専門的活動を行う国際機関のひとつであり、国際貿易に従事する海運に影響のある全ての種類の技術的事項に関する政府の規則及び慣例について、政府間の協力のための機構となり、海上の安全、効率的な船舶の運航、海洋汚染の防止に関し最も有効な措置の勧告などを行うことを目的として設置。
- ▶ IACS (International Association of Classification Societies : 国際船級協会連合) は、海上の安全の向上及び海洋環境の汚染防止に向かって活動すること、関連する国際的及び国家的な海事組織との情報交換及び協調の場を提供し、世界の海事産業と緊密な協力を行うことを目的として1968年に日本海事協会を含む7の船級協会 (ABS、BV、DNV、GL、LR、NK、RINA) で創設。

船級協会とは

- 世界の主要海運国では、中立的な立場で船舶を検査し等級付けを行うために船級協会（Classification Society）を組織し、船体や機関その他の設備に関する基準を定め、基準に合致した船舶に対して船級と呼ばれるランクを与え、船名を登録船名録に掲載。
- 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（NK）が、船級協会としての業務を行っている。



船舶のサイバーセキュリティに関する動向

- 
- ▶ IMO
 - ▶ BIMCO
 - ▶ 各船級協会におけるサイバーセキュリティ
 - ▶ NIST Framework/800シリーズ



IMO MSC (Maritime Safety Committee)

IMO FAL (Facilitation Committee)

- 海上安全委員会（MSC：Maritime Safety Committee）は全ての加盟国で構成され、2年間に3回開催されます。任務は、①航行援助、②船舶の構造・設備、③安全の見地からの配員、④衝突防止のための規則、⑤危険貨物の取扱い、⑥海上安全に関する手続き・要件、⑦水路情報、⑧海難調査、及び⑨その他の海上の安全に直接影響のある事項の検討等を行うことです。なお、詳細な検討は下部の小委員会に付託している。
- FAL委員会（Facilitation Committee：簡易化委員会）は、船舶の入出港に関わる手続きの簡易化、標準化に取り組む。

IMOにおけるサイバーセキュリティ

MSC 94 (2014年11月)

- 海事分野においてサイバーシステムへの依存が劇的に増加していることを踏まえ、船舶、港湾、海洋設備を保護するため、また潜在的なサイバーシステムの脆弱性に関する情報を共有するために、サイバーセキュリティの専門家と運航管理者の連携を強固にするサイバーセキュリティガイドラインの策定について提案。

MSC 98 (2017年6月)

- 海事サイバーリスクマネジメントのガイドラインはMSC及びFALの合同回章（MSC-FAL.1/Circ.3 : Guidelines on maritime cyber risk management）として承認された。
- 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、船主及び運航者は、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。

ガイドラインの概要（1）

(1) 目的

海運事業者に対しサイバーマネジメントの実施を促し、サイバー脅威や脆弱性に取り組めるようにするための基礎情報を提供する。

(2) 脆弱なシステム（サイバーセキュリティが必要なシステム）の例

- 船橋内システム
- 荷役システム及び管理システム
- 推進機関管理システム及び電力制御システム
- 出入管理システム
- 旅客サービスシステム及び旅客管理システム
- 旅客用公共ネットワーク
- 船上管理者システム及び船員福利厚生システム
- 通信システム

ガイドラインの概要（2）

(3) サイバーリスクマネジメント

- 海事分野においてサイバーシステムへの依存が進んでいることから、サイバー空間におけるリスクマネジメント（サイバーリスクマネジメント）が必要である。
- サイバーリスクマネジメントの目標は、運航においてサイバーリスクに対し耐性のある、安全で確実な運航を支援することである。
- サイバーリスクマネジメントは、経営陣のレベルから始まり、組織全体にサイバーリスクを周知する習慣を浸透させるべきである。
- サイバーリスクマネジメントの策定にあたり、以下の要素を含むことが望ましい。

特定：サイバーリスクマネジメントに対する個人の役割及び責任を明確にし、妨害を受けたときに船の運航にリスクをもたらすシステム、財産、データ、性能を特定すること。

保護：リスク制御のプロセス及び対策、並びにサイバーイベントから保護するためのリスク軽減計画を実施し、継続的な運航を確保すること。

検知：サイバーイベントをタイムリーに検知するために必要な行動を検討し、実施すること。

対処：回復力を備え、船の運航に必要なシステムやサイバーイベントにより害されたサービスを復元するための行動及び計画を検討し、実施すること。

復旧：サイバーイベントの影響を受けた、船の運航に必要不可欠なシステムをバックアップし、復元するための対策を策定すること。

BIMCO (ボルチック国際海運協議会)

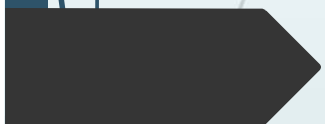
- ボルチック国際海運協議会、1905年に発足の“The Baltic and White Sea Conference”が前身。メンバーは、船舶代理店を含むブローカーの他、PI保険等を含む「クラブメンバー」や船級協会や海事法律事務所、損保や銀行等海運に関心のある「準メンバー」により構成されている。BIMCOの事業としては、傭船契約等書式の標準化が有名。IMOに対して意見を開陳する。各種外航海運データ、情報を発信している。
- BIMCOは船内システムおよびネットワークへの無許可アクセス、または悪意ある攻撃リスク等のサイバー脅威が近年大きくなっている事を受け、これらのリスク回避、もしくは低減に向けて、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」を発行している。本ガイドラインは、船主及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、業務評価方法及び必要な手順と処置の実行方法が提示されたものである。本ガイドラインは2017年に第2版が発行された。

各船級協会におけるサイバーセキュリティ

NIST Framework/800シリーズ

- 近年の船陸通信を利用した船陸間の接続性向上や船内機器統合化の推進に伴い、サイバーセキュリティに関する脅威が増大しており、これを受けて業界内でもIMO MSC(98)における規格制定や各機関からの新たなガイドライン発行等、様々な動きが見受けられる。
- まず、サイバーセキュリティ対策は大きく運航船を対象とした「サイバーリスクマネジメント」と新造船を対象とした「サイバーレジリアント船」の2つに区分できる。
- IMO MSC 98で制定された船のサイバーリスクマネジメントのSMS (Safety Management System) への記載は運航船を対象とした規格であり、このガイドラインに相当するのがBIMCOから発行されている「THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS」となる。
- IACSではCyber System Panelにおいて船のサイバーセキュリティに関して審議がされており、審議結果は運航船、新造船の双方に影響するものと考えられる。一部の船級協会は、各船級のガイドラインに沿ったセキュリティテストが実施され、サイバーレジリアントシップの認証を得る仕組みが既に構築されている。
- 各ガイドラインは最終目的が異なるものの、全てNIST Framework、即ちNIST800シリーズとの整合性を考慮して実施項目が整理されており、NIST800シリーズが参照しているIEC62443シリーズ、ISO/IEC27000シリーズ等と合わせて、船のサイバーセキュリティ対策におけるガイドラインのベースになっている。

日本における取組み





海事におけるサイバーセキュリティ タイププロジェクト

- 2016年より、サイバーセキュリティに関する国際動向をタイムリーかつ的確に把握するとともに、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・問題点を分析し、我が国海事関係者の実態に即したセキュリティ対策案を検討することを目的としてサイバーセキュリティプロジェクトを業界横断で進めている。本プロジェクトの成果を踏まえ、適宜、IMO等における各種ガイドラインの審議に貢献する。
- （一財）日本船舶技術研究協会の調査研究として「2018年度海事分野におけるサイバーセキュリティ対策に関する調査研究（サイバーセキュリティプロジェクト）」が活動中である。

SMS マニュアルへの指針作成

- サイバーセキュリティ対策におけるケーススタディとして、ISM Code (SMSマニュアル) へのサイバーリスク対応の記載を事例に、具体的な対応方法の検討を実施
- 2017年6月のIMO/MSC 98での米国提案(IMO/MSC 5/2:The incorporation of Cyber Risk Management in Safety Management Systems)に基づき、ISM Codeの中にサイバーリスクを位置付け、2021年1月1日以降の最初のSMS(Safety Management System)の改定時の認証において、SMSマニュアルに記載されていることが推奨されている。
- 船主は、この状況に今後対応が求められるが、どの程度の対策をとることが、最低限求められるかが明らかではない。SMSマニュアルのテンプレート作成作業を共同で企業横断のプロジェクトで取り組んでいる。



USCG(米国Coast Guard)

- ▶ 旗国によるSMSの審査や、寄航国における検査(PSC)の中でも、特に、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Coast Guard (USCG)が、こういったレベルの対策を求めるかを理解することが非常に重要であると考えことから、今年度については、過去の調査を通して、最もUSCGの考え方に通じていると考えられる、米国船級協会(ABS)の協力を得て進めている。



まとめ

- 海事業界全般について紹介した後、船舶のサイバーセキュリティに関する動向について述べた。
- また、動向を踏まえたうえで日本における取組みについて紹介した。



Thank you

- 本資料には日本財団の助成事業である（一財）日本船舶技術研究協会の「2018年度海事分野におけるサイバーセキュリティ対策に関する調査研究（サイバーセキュリティプロジェクト）」の成果が含まれます。本資料の作成に当たり、関係各位のご尽力に対して深く感謝申し上げます。