Vol.2020-DPS-182 No.10
Vol.2020-CSEC-88 No.10
2020/3/12

自動操船システムのゾーニングによるセキュリティアーキテクチャの提案

小林英仁 [1*]　松井俊浩 [1]

概要：将来の自動運航船がセキュリティ上の脅威にさらされても安全に運航するためのゾーン型の自動操船システムアーキテクチャを提案する．外洋船の自動運航では，サイバーセキュリティの脅威にもさらされることから，目的地までの効率的な大域航路の計画のような上位タスクよりも悪天候回避，衝突回避，座礁回避，遠隔制御の実行，機関やリソースの保護，安全な接岸，安全な停船のような安全システムを強く保護する必要がある．これらは，多数のセンサと情報系，ソフトウェアをネットワークするが，安全システムは階層的に組み立てられるべきであることから，これらの情報系もゾーニングによって分離して安全を確保する必要がある．本論文では，これらの自動運航船の機能要求・安全要求を分析し，その実現に適したゾーニングアーキテクチャを提案する．提案アーキテクチャを用いることで GPS ジャミング及び GPS スプーフィングが操船システムの中核機能に及ぼす影響を軽減できるとともに，荒天回避や輻輳海域回避，避航，保針・船体揺動抑制の各機能のマルウェア感染に起因する異常動作を検知できる．

キーワード：自動運航船，操船システム，セキュリティ，ゾーニング，船舶

Proposing a Security System Architecture of Autonomous Ships Maneuvering System

HIDEHITO KOBAYASHI[1*]　TOSHIHIRO MATSUI[1]

Abstract: This This paper proposes a zone-type automated ship maneuvering system architecture for safe operation even if future automatic ships are exposed to security threats. Since ocean-going vessels are also exposed to cybersecurity threats, they avoid bad weather, avoid collisions, avoid grounding, perform remote control, and perform higher-level tasks such as efficient global route planning to the destination. Safety systems such as engine and resource protection, safe berthing, and safe berths need to be strongly protected. These network many sensors, information systems, and software, but safety systems should be assembled hierarchically, so these information systems must also be separated and secured by zoning. In this paper, we analyze the functional requirements and safety requirements of these automatically operated ships and propose a zoning architecture suitable for the realization. By using the proposed architecture, the effects of GPS jamming and GPS spoofing on the core functions of the ship maneuvering system can be reduced, and abnormal operations caused by malware infection in the functions of avoiding stormy weather, avoiding congested sea areas, evacuating, and keeping hands and swaying can be detected.

Keywords: Autonomous Ship, Maneuvering System, Zoning, Security, Ship

1. はじめに

海自業界では長年にわたり，年々高まる船員需要の逼迫や船員作業負担の増加等の課題に取り組むことが求められているが，特に近年の海上ブロードバンド技術やセンシング技術，AI，センシング技術，ビッグデータ技術等の急速な発展を受けて，自動運転技術を取り入れた船舶（自動運航船）の実現に大きな期待が寄せられている．自動運航船の研究は 2012 年頃より特に欧州で勢力的に行われてきており，研究開発の初期には概念構築を目的としたプロジェクトが発足したが，実システムの構築や実証実験を行うものは見られなかった．しかし，2018 年 12 月には英海事大手ロールスロイス社らによって世界初の自律運航型フェリーが発表されるなど，近年になり研究成果が実社会のサービスとして現れつつある．

従来の船舶では，航海計器や主機制御装置，無線等通信機器等の各機器はそれぞれがスタンドアローン形態あるいは最低限の接続形態で船内に組み込まれ，機器毎に限定された利用用途や運用シナリオの中で有人操船を支援するために用いられる．一方で自動運航船においては航海系統，主機・推進系統，無線等通信系統等の各系統の機器が互いに接続され，運航環境認識や状況判断・意思決定，行動，の一連のプロセスが自動化されるとともに有人乗組員や陸上オペレータはそれらを監視監督し必要時にのみ操船システムの動作に介入するものになると考えられる．その際，目的港や航海日程，その他船舶運営会社から与えられたオペレーション条件を満たすよう航海計画を自動的に立案することはもちろん，航海時の事故や自船にとって望ましくない事態に適切に対処することが求められる．

自動運航船に対するサイバー攻撃は，その攻撃による影響が船舶の座礁や衝突といった人命・船体の安全性を脅かす深刻な事故を引き起こす可能性がある．本研究では，サ

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

* mgs185505@iisec.ac.jp

Vol.2020-DPS-182 No.10
Vol.2020-CSEC-88 No.10
2020/3/12

イバー攻撃にさらされても安全かつセキュアな運航プロセスを行うことができる自動操船システムアーキテクチャの提案を目的とする．

2. 先行研究

MUNIN（Maritime Unmanned Navigation through Intelligence in Network）プロジェクト[1]は，ドイツとりまとめのもと北欧諸国を中心とする各国研究機関，大学，企業等が参画し，経済効率性の高い無人ばら積み船の概念構築とそのための実証実験を目的として実施されたプロジェクトである．MUNIN プロジェクトでは輻輳海域における自律操船や出入港作業には法制度上の解決課題や困難な技術課題が存在することに言及するとともに，輻輳海域を避けた特定の航行区間においてのみ自律操船による航行を行い，出入港作業や輻輳海域における操船は有人乗組員が手動で行うことによる手動/自動操船切替型の運航モデルを提示した．同プロジェクトにて Rødseth ら[2]は，計測器層やプロセス層，統合制御層等の複数の階層から構成される船舶ネットワークモデルを示した．

MUNIN プロジェクトでは，船舶の安全運航を実現するためのリスクアセスメント結果が提示されたものの，特にサイバーセキュリティ上の脅威とその結果発生する恐れのあるインシデント，またそれらの対策として検討すべき防護措置について必ずしも十分な考察がなされていない．自動操船システムのアタックサーフェスとして衛星通信リンク，センサ類，船内 LAN 接続機器等が挙げられるが，これらに対するサイバー攻撃の脅威として例えば衛星通信リンクを介したインターネットからの不正アクセスや GPS ジャミング，スプーフィング，AIS（Automatic Identification System：自動船舶識別装置）通信方式の脆弱性を利用した架空情報や偽装情報の受信[3]，外部電磁的記録媒体を通じた船内 LAN 構成端末のマルウェア感染が挙げられる．

MUNIN プロジェクトにより提示されたシステムモジュール構成及び機能分類結果[4]では，システムモジュール単位で自動運航に必要な機能要素がリストアップされた．例えば，メインモジュールである自動船舶コントローラはウェザールーティングや衝突回避，航行状況認識等の機能を備えるとともに，サブモジュールであるセンサシステムやブリッジシステム，エンジンシステムでそれぞれ，自己位置推定や自動操舵，エンジンデータ提供等の機能を備えるものとされた．しかし，各モジュール内に実装される機能群について，サイバー攻撃からどの機能を優先して保護すべきかに関する考察はなく，保護優先度の異なる機能群が同一モジュール内に混在して分類されたものであると捉えられる．例として，自動船舶コントローラにおける緊急警報の機能は，人命保護や船体損傷防止の観点から，ウェザールーティングのような大域的な最適航路計画よりも機能異常や不具合を優先して予防・保護すべき性質の機能であると考えられる．

3. 自動運航機能要素のゾーニングによる操船システムアーキテクチャ

3.1 アーキテクチャ概要

自動運航船はひとたび出港すれば長期間洋上で孤立することとなり，操船システムに対するサイバー攻撃を検知，防止するために利用できるシステムリソースには限界がある．自動運航を行うために操船システムが備えるべき機能に着目すれば，これらの機能自体がサイバー攻撃から保護すべき情報資産である． 提案手法では，限られた船内リソースでサイバー攻撃から効果的にこれらの機能を保護することができるよう，ゾーニングを行い，より重要な機能を構成する機器を優先して保護するものとする．

自動運航を実現するための機能をゾーニングし，重要度の高い機能を構成する機器を優先して保護することができるよう，自動操船システムを構成するためのアーキテクチャを示す．自動運航のために求められる機能要素を以下の３つのレベルに分類する．

- 最重要層（第１層）：人命・船体安全保護層
  船内火災や浸水等の人命や船体に直接的な危害を及ぼす事故に対処するために必要な機能群が本層に位置付けられる．これらは自船が事故に直面した際に必要となる機能であり，機能障害の発生が最も優先して防がれなければならない．
- 高重要層（第２層）：航海安全保護層
  他船や環境と干渉することなく安全に航海するために必要な機能群が本層に位置付けられる．本層には主に，他船が安全距離を越えて自船に接近するように，わずかな時間猶予や自船の近傍で想定されるハザードに対処するために必要な機能群であり，他船との衝突や座礁等の事故を予防するために保護されるべきである．
- 低重要層（第３層）：最適オペレーション層
  悪天候回避や海上交通輻輳海域回避等の大域的な安全性あるいは経済性を向上させるために必要な機能群が本層に位置付けられる．

図１に自動運航方式を実現するために必要な機能要素のゾーニングイメージを示す．各機能を，前述の３つの層のいずれかに分類するとともに，最重要層である人命・船体安全保護層から順に，航海安全保護層，最適オペレーション層の順に優先して保護することができるよう実システムモデルを構築するものとする．各層は，それぞれの機能を実現するための機器群で構成し，各層間は FW（ファイアウォール）で接続する．FW では優先度の低い層からより優先度の高い層への通信内容の監視を行い，悪性通信が検出された場合には通信を遮断することにより，より優先度

Vol.2020-DPS-182 No.10
Vol.2020-CSEC-88 No.10
2020/3/12

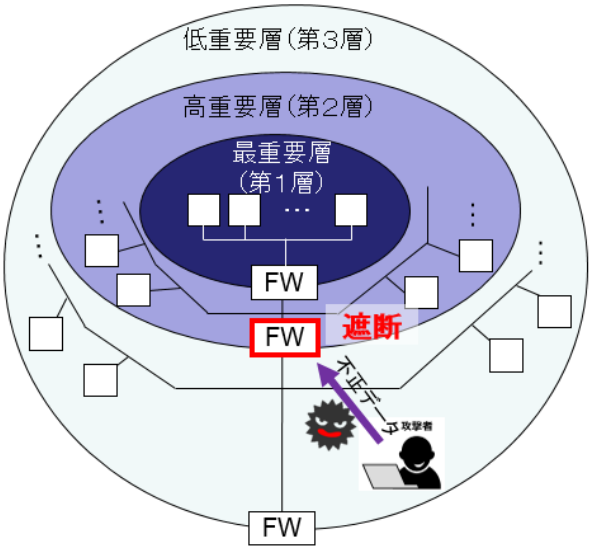

図 1　低重要層から伝送された不正通信の遮断による
高重要層機能のサイバー攻撃保護のイメージ

の高い層を構成する機器群がサイバー攻撃によって不正動作することを防ぐことができる．同図は低重要層ネットワーク内に侵入した攻撃者から送信された悪性通信を層間 FW で遮断する際のイメージが示されている．

層間 FW で悪性トラフィックが検知された場合，トラフィック送信元の層内の他の機能も正常動作していない可能性が疑われる．また攻撃者が侵入したネットワークセグメントを基点として同層内の各機器にマルウェア感染や横展開侵入されることにより機能障害の範囲，深刻さが拡大することが考えられる．そのため上記で述べたような悪性通信の検知や遮断処理に加えて，各層内各機能の正常性を定期的に監視・診断するとともに機能異常時には FW に対して層間通信の遮断を命令する仕組みが必要である．なお異常動作が検出された機能については，有人乗組員により手動制御を行うこととする．自動運航に必要な機能要素のゾーニング結果を表 1 に示す．

以降の節では各層に位置付けられる機能要素の処理内容と関連機器間データフローを示す．特にデータフローに関して，MUNIN プロジェクトにより提示されたフローマップ[4]は各機能の入出力となる情報や情報源となる機器が抽象的な形式でモデル化されており各機能の制御部（以下，コントローラと呼ぶ）に対して具体的にどの機器との入力/出力データフローが発生するのかが不明瞭である．これに対して本稿では，実機器及びデータの内容を明確化した形で各機能の処理内容及びデータフローを示す．

3.2　人命・船体安全保護層に位置付けられる機能要素

火災安全機能は，火災検知及び船内警報を発する監視システムと消火を行う消火システムで構成される．機関室や居住区などの区画毎に熱・煙感知器，手動火災発信機，ベル等が設置され，センサによる感知に加え，有人乗組員が直接，手動火災発信機を作動させることによって火災受信

表 1　自動運航に必要な機能要素のゾーニング結果

層名	機能名
人命・船体安全保護層	火災安全，水害安全，救助要請，錨泊，主機停止，非常発電，自己診断，統合自己診断
航海安全保護層	避航，保針，船体揺動抑制，設定船速維持，主機負荷一定制御，船速変更（CPP 制御），旋回，軸発電，走錨防止，自己診断
最適オペレーション層	荒天回避，輻輳海域回避，自己診断

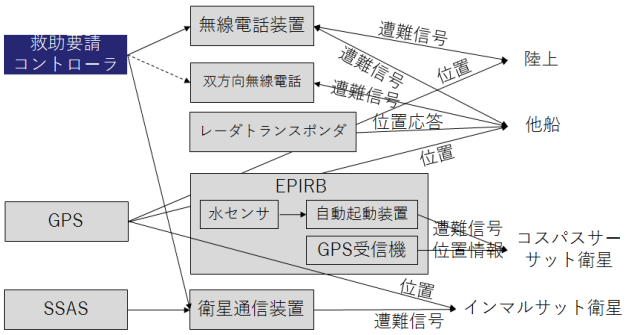

図 2　救助要請に関するデータフロー

機に火災発生が通知されるとともに火災区画のベルが鳴動する．監視システムは自動で，あるいは，有人パネル操作により手動で，消火システムに対する消火命令を発信する．消火システムとしてここでは，あらかじめ貯蔵された水あるいは炭酸ガスを火災発生区画の固定噴射ヘッドから噴射して消火する方式を想定している．貯蔵容器と噴射ヘッド側制御装置のそれぞれの弁が開放されることで，あらかじめ貯蔵された水または炭酸ガスが噴射される．

火災安全機能と同様に，水害安全システムは災害検知，船内警報，及び災害対処を行うサブシステムによって構成される．区画毎に浸水センサ，手動浸水発信機，ベル等が設置される．センサによる感知に加え，有人乗組員が直接浸水発信機を作動させることによって受信機に水害発生が通知されるとともに水害区画のベルが鳴動する．監視システムは自動で，あるいは，有人パネル操作を介して手動で，排水システムに対して排水命令を発信する．排水システム内では，バルブの電気制御によって排水処理が行われる．

救助要請機能は，海難時の救助要請に関する世界的制度である GMDSS（Global Maritime Distress and Safety System：海上における遭難及び安全に関する世界的な制度）により搭載義務が規定された特定の無線等通信設備により構成される．図 2 に本機能に関するデータフローを示す．なお救助要請コントローラは，各機器に遭難信号の発出を命令する機器であるものとする．救助要請機能はコントローラによる自動送信以外に乗組員が手動で SSAS（Ship Security Alert System：船舶保安警報発信装置）を操作することでもトリガーされる．本機能は主に船内火災，浸水，沈没，衝突，座礁，ハイジャック，物資略奪（海賊行為）等の状況で作動するものであるが，救助要請時には生存艇の場所を

Vol.2020-DPS-182 No.10
Vol.2020-CSEC-88 No.10
2020/3/12

知らせるための自船位置情報の付加が極めて重要である．そのため陸上，他船あるいは各衛星に対して遭難信号を発出する機器は機器本体内外に位置情報を取得するための機器を参照できるよう相互接続されていなければならない．すなわち，GPS 受信器から参照した位置情報を併せて救助要請先に伝達するためのデータフローが発生する．

錨泊機能は，船体損傷や機関異常により正常な移動能力が失われるとともに救助を待つ際に，漂流を防ぐために洋上停泊する場合の利用を想定している．一般に錨泊中の事故として，走錨による漂流の結果，座礁や乗り上げを起こすことが知られている．松永[5]は，自船が本来の移動能力を有するという前提のもとで，投錨，守錨，揚錨の一連の作業を自動で行うための錨泊システムの概念を示した．同文献では，投錨，守錨，揚錨のプロセス毎にサブシステムを構成することで乗組員の介在なしに錨泊作業を行うためのシステムの概念が示された．この方式に基づく場合の錨泊機能に関するデータフローを図 3 に示す．投錨時には，走錨予防のための適切な錨泊地の選定のために，水深や海底地形の情報を取得する必要がある．これらの情報はソナーあるいは ECDIS（Electronic Chart Display and Information System：電子海図表示装置）内に保存された電子海図から取得される．投錨プロセスは自船の運動が十分に低速となった段階で実行することが望ましく，船速計の値が一定値以下となった時点で投錨することで安全に同プロセスを行うことができる．投下作業は，錨鎖制御装置内の揚錨機アクチュエータに対して降錨命令を送信するとともに，アンカー力センサで検知される錨張力の値を監視することにより進められる．守錨に関して，一般に走錨予防措置として錨鎖を延ばすことで錨鎖と海底面との摩擦抵抗が増加し把駐力が向上することが知られている．すなわち，守錨時にはアンカー力センサで検知された鎖張力の情報にもとづきアクチュエータを適切な錨鎖長となるよう制御するデータフローが発生する．なおここでは自船の推進機関に異常が発生し正常な移動能力が失われている場合を想定しており，一般の走錨時措置として採られるように主機や舵，スラスタを用いた振れ回り運動の抑制制御はここでは考慮しない．

主機停止機能は，船内火災，浸水等によって主機運転状態に異常が検出された場合に速やかに主機を停止するためのものである．

非常発電に関連して，平常運航時の船内電力の発電方式として例えば排ガスタービン発電や軸発電等の方式が採用されるが，ここでは主機及び推進器等が十分に機能せずこれらの方式による発電を効果的に行うことができない場合を想定する．非常発電機能は，本機能以外の最重要層機能が正常に稼動されるよう，人命・船体安全保護層機能を構成する各機器に対する電力を供給するための機能である．

自己診断機能は，同層内に位置付けられる機能を構成する各コントローラが正常に動作しているか否か判定するための機能である．同層内の各コントローラは，自己診断コントローラから検査内容を受信した後，検査実行結果を同コントローラに応答する．自己診断によって，（1）各コントローラに対する不正な情報入力の有無や（2）各コントローラ内演算処理の整合性が判定される．第（1）項の検査によって各コントローラに対する不正な情報入力が確認された場合にはすなわち，攻撃者による不正な情報の注入が疑われる．また第（2）項の検査によって自己診断コントローラの演算処理結果が不正でないことを検査することにより，不正なコードやデータの注入等によりコントローラが異常動作していないことを監視するものである．なお航海安全保護層と最適オペレーション層の同名機能についても同様の手順により同層内コントローラの診断を行うものとする．

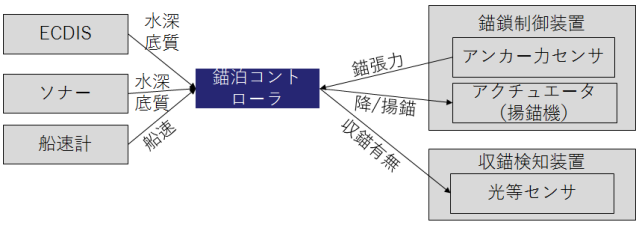

図 3 錨泊に関するデータフロー

自己診断によるコントローラ機能の正当性は，当該検査情報を生成，送信する自己診断コントローラ自身が正常に動作していることが確認できなければならない．統合自己診断機能は，各層の自己診断コントローラ群についてそれらが正常に動作していることを検査するための機能である．特に，いずれかの機能層がサイバー攻撃によって動作不良に陥った場合にそれを検知するためには同層の自己診断コントローラより重要度の高い層，すなわち，より優先的に保護されるべき層にて自己診断の正当性を保障する必要があることから構成するものである．

3.3 航海安全保護層に位置付けられる機能要素

避航機能は，自船が他船や浮標物とあらかじめ定めた距離よりも接近した場合に，それらとの衝突を避けるための操船を行う機能である．なお岸壁や浅瀬，暗礁に接近した場合に，それらとの衝突，乗り上げ，座礁を避けるための操船についても本機能に含める．図 4 に，本機能に関するデータフローを示す．GPS 受信機，船速計，姿勢センサから自船運動情報が，AIS，可視カメラ，赤外線カメラ，レーダから他船運動状態が，レーダ，ECDIS から航行環境地形（岸壁情報等）が，ECDIS，ソナーから水深情報が，それぞれ取得され避航コントローラへ渡される．コントローラは，渡された情報から衝突予測を行い，回避するための予定航路を計画し，同航路上を追従するように推進・操舵系システムへ避航操船を命令するものとする．衝突予測にもとづく避航操船方法に関して文献[6]では，OZT（Obstacle Zone by Target：目標による障害ゾーン)[7]に基づく避航操

Vol.2020-DPS-182 No.10
Vol.2020-CSEC-88 No.10
2020/3/12

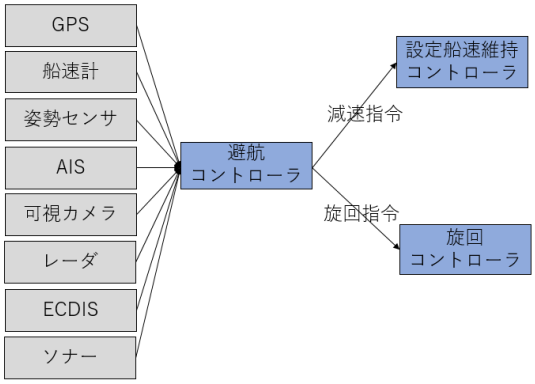

図 4　避航に関するデータフロー

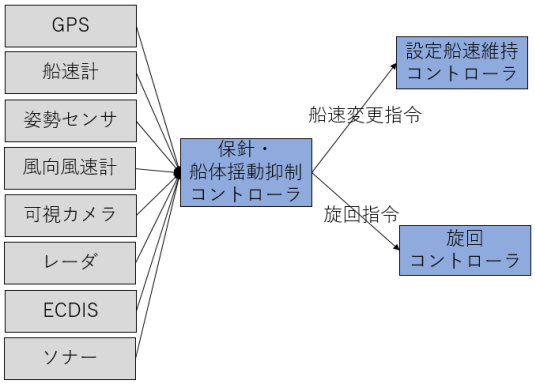

図 5　保針・船体揺動抑制に関するデータフロー

船シミュレーション結果が示された．これらの成果を参考にし，避航コントローラは設定船速維持機能コントローラへ減速指令を，また旋回機能コントローラへ左・右旋回指令を，それぞれ出力するものとする．なお自船速度を増加させることによる衝突回避は考えないこととする．

船速変更は，主機の目標回転数を変更することによる方法と CPP（Controllable Pitch Propeller : 可変ピッチプロペラ）の翼角を変更することによる変更とが考えられるが， CPP 翼角変更方式を採用した場合の停船性能や船速調節性能の高さから，主機回転数を一定に維持したまま CPP 翼角設定を変更することにより船速を変更するものとする．

保針機能及び船体揺動抑制機能は，強風や風浪等の影響を受けた場合にも船体動揺を抑制するとともに計画された予定航路上を逸脱することなく追従するための機能である．荒天時の操船等では，強風や風浪により船体が上下方向，縦方向，横方向のそれぞれに揺れるとともに，風，波により生じる抵抗によって速力が低下する．揺れの影響を抑制，軽減しない場合には，例えば上下揺れによりプロペラの一部が周期的に海面から露出しプロペラ機構を損傷させるレーシング現象や，目標船速を出力するようエンジンに過負荷がかかりエンジンを損傷させるトルクリッチ現象が発生する．このような環境化での操船時には一般に，外力の影響を相殺するよう風，波の方向に直行するように操舵したり目標船速値を小さく設定し低速で航行したりする等の措置が有効であるとされている．また波検知に関して平山[8]は，レーダ画像情報から方向波スペクトルを解析することにより異常波浪を直前で検知できることを示した．以上を参考に本機能を構成する場合のデータフローを図 5 に示す．GPS，船速計，姿勢センサからは自船運動状態が，レーダ，ソナーからは潮流情報が，風向風速計からは風速情報が，それぞれ取得される．保針・船体揺動抑制コントローラは上記で述べた操船方針にもとづき潮流，風の影響による揺動，速力低下の影響を軽減することができるよう，目標の自船運動状態を算出するものとする．同コントローラから CPP 制御コントローラへ翼角減少が命令されることで目標船速の低下が，また同コントローラから旋回コントローラへ左右旋回が命令されることで外力による揺動の軽減が，それぞれ行われるよう構成するものとする．

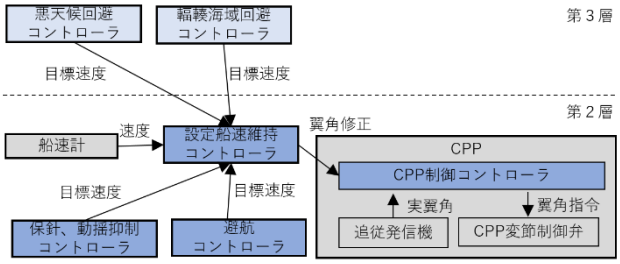

図 6　設定船速維持に関するデータフロー

設定船速維持機能は，他機能によって算出された目標の船速値と実際の船速値が異なる場合に，CPP 翼角を変更し実船速を目標船速に近づけるよう制御するための機能である．一般に設定船速維持の方式として，CPP 翼角一定のもとで主機回転数を調節することによる方法と，主機回転数を一定に維持したまま CPP 翼角を調節することによる方法とが挙げられるが，前述の通り CPP 翼角調節による速度変更方式の方が主機回転数調節による速度変更方式よりも操船性能上の利点を有することにより，本機能も前者の方式により制御するものとする．図 6 に本機能に関するデータフローを示す．目標船速値は避航コントローラや保針・船体揺動抑制コントローラのほか，最適オペレーション層の機能によってそれぞれ計算されるため，いずれのコントローラが算出した値を優先し最終的な目標値をどのような値とするべきかについては，船体の動揺や減速によって船体やエンジン，プロペラ等各機関が損傷しないよう考慮すべき安全性の度合いにしたがって，本コントローラ内で決定されることが必要である．

主機負荷一定制御機能は主機にかかる負荷をあらかじめ設定された目標負荷値に近づけるよう CPP 翼角を制御する機能である．本機能により主機回転数一定とし翼角値を変更することにより主機が過負荷領域や低負荷領域で運転しないよう目標の翼角値が算出される．主機負荷一定制御コントローラは主機から負荷情報を含む運転情報を，CPP 制御コントローラから CPP 翼角実値を，それぞれ取得

Vol.2020-DPS-182 No.10
Vol.2020-CSEC-88 No.10
2020/3/12

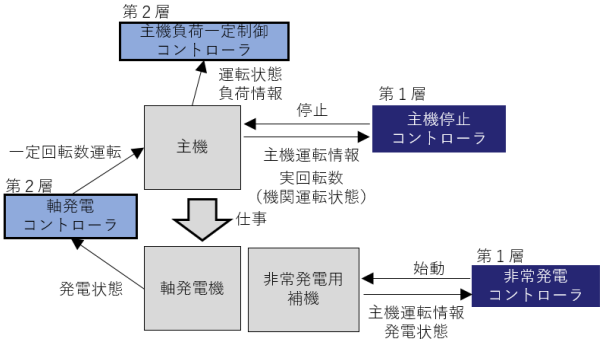

図７　発電系統に関するデータフロー

した後，過負荷や低負荷を避け望ましい負荷を実現するための翼角目標値を算出するものとする．その際，設定船速維持コントローラでも翼角目標値が計算されるため，どちらのコントローラが算出した値を優先し最終的な目標値をどのような値とするべきかについては目標船速値の優先度合い，主機に許容される負荷の度合い等にしたがって，両コントローラ間で目標船速値と目標翼角値の決定に関する調停が行われることにより，決定されなければならない．

軸発電機能は，平常運航時に主機を一定回転数で運転することにより船内系統に電力供給するための機能である．船速変更を CPP 翼角調節によってのみ行うよう制御することで，周波数変動のない電力供給が期待される．軸発電コントローラは主機に対して回転数一定で運転するよう制御を行う．軸発電機は電力を船内系統に供給するとともに，軸発電コントローラに対して発電力量や周波数等に関する発電情報を送る．図７に，発電系統及びエンジン系統に関するデータフローを示す．

3.4 最適オペレーション層に位置付けられる機能要素

荒天回避機能は，気象海象情報にもとづき悪天候や台風等の荒天に遭遇しない予定航路を計画するとともに運航を行うための機能である．図８に本機能のデータフローを示す．ナブテックス受信機，気象 FAX 受信機及びインターネット上サービスにより気象海象情報がコントローラへ送られる．GPS 位置情報，船内 LAN 端末により乗組員に指定された目的港情報あるいはインターネット経由で船舶運航会社等から入力された目的港情報とともに，コントローラ内で悪天候を避けつつ現在位置から目的港へ到着するための予定航路が計画される．予定航路にしたがって第２層の設定船速維持コントローラ及び旋回コントローラに対して船速増加/減少指令及び左右旋回指令が送られる．

輻輳海域回避機能は，他船との干渉・衝突を避けることができるよう輻輳海域を避けて目的港へ到着するための予定航路を計画，運航するための機能である．図９に本機能のデータフローを示す．インマル衛星通信を介してインターネット AIS サービスプロバイダの提供する船舶運航情報が，またナブテックス受信機から海上交通量の増加や航行警報等に関する情報が，それぞれコントローラへ送られる．

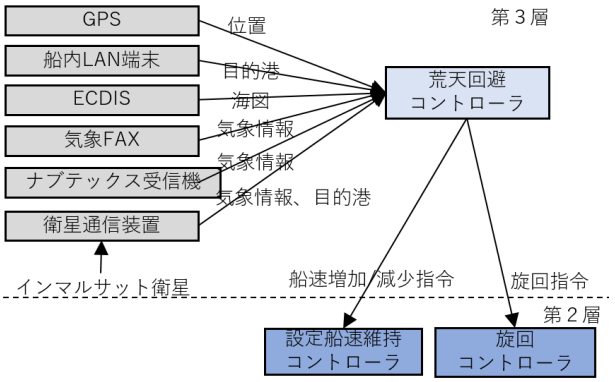

図８　荒天回避に関するデータフロー

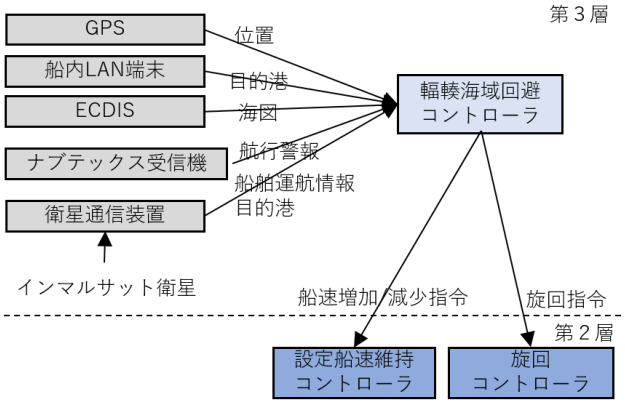

図９　輻輳海域回避に関するデータフロー

4. 層間異常伝送データの検知と遮断によるサイバー攻撃の影響の緩和

4.1 GPS ジャミング

GPS 受信機により得られた自船位置情報は提案システムにおける各層でその値がコントローラへの入力として用いられる．そのため，GPS ジャミング攻撃によって受信機から位置情報が得られない状況に陥った場合には，攻撃の影響が各層に伝播する可能性があるとともに，機能保護重要度の低い層の機能不具合に起因してより機能保護重要度の高い層の機能不具合が誘発される状況が発生することが考えられる．なお市販 GPS 受信機のハイエンドモデルでは，GPS 衛星信号が受信できない場合に GLONASS 衛星やみちびき衛星等の他の衛星信号を用いるマルチ衛星測位機能や加速度・角速度の値から位置を推定する自律航法（デッドレコニング）機能を備える製品が存在する．このような受信機個別のジャミング対策が利用できることを前提として，提案システムにおけるコントローラ動作を以下のように設計することによりジャミング影響の層間伝播を軽減することができると考えられる．

最適オペレーション層の荒天回避機能及び輻輳海域回避機能は，いずれも大域的な航路計画を行うために自船位置を含めた速度や姿勢等の自船運動状態を入力として参照す

Vol.2020-DPS-182 No.10
Vol.2020-CSEC-88 No.10
2020/3/12

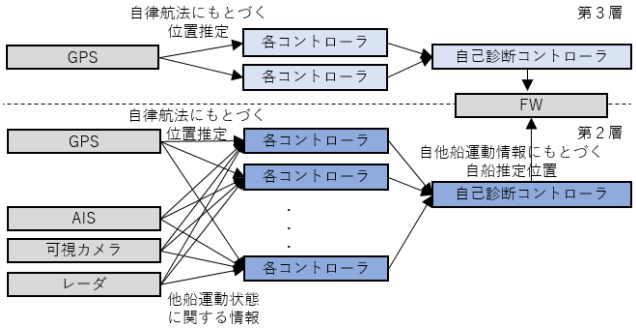

図 10　GPS ジャミングの検知と層間伝播緩和

る．これに対して航海安全保護層の避航機能や保針・船体揺動抑制機能は自船運動に関する同様の情報に加えて，AIS や可視カメラ，レーダから取得された他船運動に関する情報を入力され利用可能である．したがって，航海安全保護層において GPS 位置情報が入力として渡されるコントローラの中で位置以外の自船運動情報を用いたデッドレコニングによる自船位置推定を行うとともに，他船の位置・速度等の情報にもとづき両船の相対運動情報から自船位置推定精度の向上を図ることで，ジャミング時にも最適オペレーション層より高い精度で位置を推定することができると考えられる．両層で算出された位置情報を層間 FW で比較し，一定以上の誤差がある場合にはジャミングが発生したと判断する．図 10 に本方式のデータフローイメージを示す．

4.2 GPS スプーフィング

GPS スプーフィングによる位置情報の改ざんについても，GPS ジャミング対策の節で述べた方法と同様の位置推定を最適オペレーション層と航海安全保護層のそれぞれで行い，両者の推定値を比較することにより攻撃発生の有無を判定できると考えられる．ただしスプーフィング時には GPS 受信機本体のデッドレコニング機能は正常に動作しないことが考えられるため，航海安全保護層において位置以外の自船運動情報に加えて AIS やレーダ等から取得される他船運動情報を用いて自船位置推定を行うことが必要である．最適オペレーション層で GPS 受信機により取得された位置情報と航海安全保護層で GPS 位置以外の自他船運動情報から推定した自船位置情報とを比較し，両者の値に一定以上の誤差が見られる場合にはスプーフィングあるいは GPS 受信機本体の故障や動作不良が発生したものとし，GPS 位置情報参照時には自動的に他船運動情報を用いた位置推定結果をもって自船位置とみなすことが必要である．

図 11 に本方式のデータフローイメージを示す．最適オペレーション層では，スプーフィングを受けた位置信号が同受信機から同層内各コントローラへ，またそれらコントローラから同層内自己診断コントローラへ，それぞれ渡される．航海安全保護層では，船速計や姿勢センサから自船運動に関する情報が，AIS，可視カメラ，レーダから他船運動

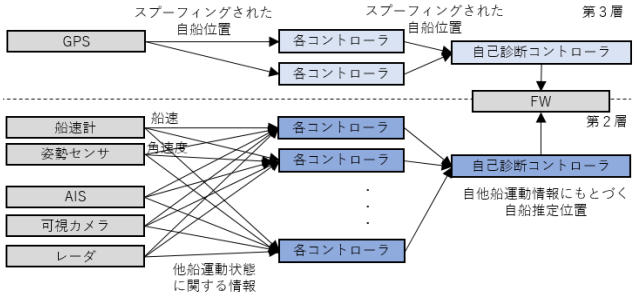

図 11　GPS スプーフィングの検知と層間伝播緩和

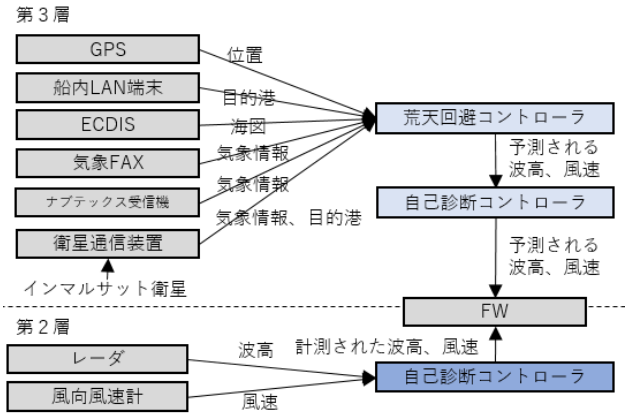

図 12　荒天回避機能の異常検知

に関する情報が，それぞれ同層内コントローラ及び自己診断コントローラに渡される．層間 FW で両自己診断コントローラから渡された自船位置が比較され，スプーフィング発生有無が判定される．

4.3 マルウェア感染による機能コントローラ異常の検知

本節では，各コントローラが外部電磁的記録媒体インタフェースを備えると仮定し，マルウェア混入した媒体がコントローラに接続されることにより感染し，当該コントローラが異常動作する場合を考える．

荒天回避コントローラの異常動作を航海安全保護層にて検出するための方法として，波浪レーダや風向風速計から取得される気象海象にもとづき自船が直面する航行環境の荒天度合いを評価する方法が挙げられる．荒天回避コントローラにおける航路計画時に自船が遭遇する波高や風速の最大許容値を定めておき全航行区間でこれらの値が超過することがないよう予定航路を計画する．一方で運航時には，船上で波高，風向風速を計測し，航路計画時に設定した最大許容値を超過していないか否かを比較判定する．計測値が計画時の最大許容値を許容している場合には，荒天回避機能が正常に動作していないものと判断し，乗組員が手動で悪天候回避するための航海計画を行うものとする．ただし気象警報の予測誤りにより航路計画時と異なる気象海象環境で運航するケースが実際にはよく見られることから，これらと荒天回避コントローラ動作異常とを区別することができるよう波高や風向風速の最大許容値は十分に大きな値とする必要があると考えられる．図 12 に本コントロー

Vol.2020-DPS-182 No.10
Vol.2020-CSEC-88 No.10
2020/3/12

ラ異常動作検出に関するデータフローを示す．

輻輳回避コントローラの異常動作の検出についても，荒天回避コントローラの異常動作の検出の場合と同様の考え方によって実現できると考えられる．すなわち輻輳回避コントローラの異常動作を航海安全保護層にて検出するための方法として，AIS，レーダから取得される他船動静にもとづき自船周囲の交通の輻輳度合いを評価する．輻輳海域回避コントローラにおける航路計画時に自船が遭遇する交通輻輳の最大許容値を定めておき全航行区間でこれらの値が超過することがないよう予定航路を計画する．なお交通輻輳度については運航時に AIS やレーダにより取得可能な情報により計算することができるよう別途定義することが必要である．運航時には，AIS，レーダ計測値より実際の交通輻輳度を計算し，計画時に設定した最大許容値を超過していないか否かを判定する．計測値が最大許容値を許容している場合には，輻輳回避機能が正常に動作していないものと判断し，乗組員が手動で輻輳海域を回避するための航海計画を行う．

避航コントローラ異常時には，あらかじめ定めた距離よりも他船や岸壁等と接近するとともに衝突や座礁を起こす危険性が増加する．ここで，他船避航が正常に行われない場合には他船から衝突回避措置を採るとともに旋回方向や速度の減速等の意思の確認と調停を行うための無線等通信を受信することとなると予想される．したがって，同コントローラの異常動作の検出として，人命・船体安全保護層の救助要請機能を構成する無線等機器の動作を監視することによる方法が挙げられる．短期間内に他船からの接近通知や回避操船依頼が頻発したり，あるいは適切な船間距離を設定しているにも関わらず他船との安全距離を大きく超過して接近したりするような状況が見られた場合には避航コントローラの動作異常が発生しているものと判断し，乗組員による手動操船に切替えることが必要である．図 13 に本方式のデータフローを示す．層間 FW によりコントローラ異常有無を判定する．

保針・船体揺動抑制コントローラ異常時には，船体の動揺を抑えることができず甲板への波の打ち込みや上下動に伴うプロペラ部の損傷等が発生することが考えられる．ここで同コントローラにおいては，CPP 制御コントローラに対して減速するために翼角調節指令のみが送られることに注目すれば，本コントローラから CPP 制御コントローラに対して船速増加する方向に翼角修正が送られた場合に動作異常が発生しているものと判断する方法が考えられる．

5. まとめと今後の課題

本研究ではサイバー攻撃にさらされても安全かつセキュアな自動操船システムアーキテクチャの提案を目的とし，操船システムが備えるべき自律機能をゾーニングすることにより，船内ネットワークを人命・船体安全保護層，航海

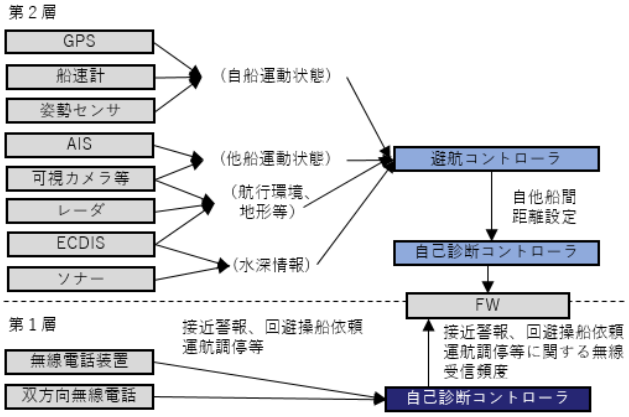

図 13　避航機能の異常検知

安全保護層及び最適オペレーション層の３層に分類するとともに各機能に関する層内及び層間のデータフローを提示した．提案アーキテクチャを用いることにより GPS ジャミング及び GPS スプーフィングの影響が最適オペレーション層からより高重要へ及ぶことを緩和することができる．また荒天回避，輻輳海域回避，避航，保針・船体揺動抑制を行うコントローラがマルウェア感染しコントローラ動作異常が発生した場合に，それらのコントローラの上位層の情報を利用して動作異常を検知することができる．

今後の検討課題として，検知された異常がサイバー攻撃に起因するものなのか機器故障に起因するものなのか切り分ける必要がある．また不審船の接近やハイジャック，権限のない乗組員による船内ネットワーク管理端末への不正アクセス等のさらなる脅威シナリオの分析を行いたい．

参考文献

[1] T. Porathe et al., “Maritime Unmanned Navigation through Intelligence in Networks: The MUNIN project,” Proc. of *the 12th International Conference on Computer and I Application in the Maritime Industries*(COMPIT’13), 2013.

[2] Ø. J. Rødseth et al., “Design challenges and decisions for a new ship data network,” Proc. of *the International Symposium Information on Ships* (ISIS), 2012.

[3] M. Balduzzi et al., “A security evaluation of AIS automated identification system,” Proc. of *the 30th Annual Computer Security Applications Conference* (ACSAC '14), pp. 436-445, 2014.

[4] W. Bruhn et al., “MUNIN D5.2:Process Map for Autonomous Navigation,” 2013，https://www.unmanned-ship.org/munin/wp-content/uploads/2014/01/MUNIN-D5-2-Process-Map-for-Autonomous-Navigation-CML-final.pdf

[5] 松永宣雄，“高信頼度知能化船（高度自動運航システム） ―（その 11）自動錨泊システム―”，日本造船学会誌，pp. 46-50，no. 727，1990.

[6] 丹羽康之，“船橋の自律化技術”，第 17 回海上技術安全研究所研究発表会，2017.

[7] 今津隼馬，福戸淳司，沼野正義，“相手船による妨害ゾーンとその表示について，” 日本航海学会論文集, pp. 191-197，no. 107，2002.

[8] 平山次清，“荒天中の安全運航の為のバーティカルタイプ・スタビライザーと波浪レーダ，”海洋回 横浜支部講演会，2015，https://www.kaiyo-kai.com/kaiyo-kai.com/wp-content/uploads/editor/File/150310_yokohamahappyo.pdf