情報セキュリティ大学院大学
情報セキュリティ研究科
修士論文

GPS ベースの船舶航海システムに対する攻撃と防御

Attack and Countermeasure for GPS-based Ship Navigation Systems

学籍番号 5505504
仙田 眞之
Saneyuki Senda

指導教員　須崎 有康

2024 年 2 月

概要

船舶の操船において，AIS や ECDIS 等の航海システムは必要不可欠であり，そこで必要となる位置情報の取得は GPS 等の衛星システムに多く依存している．

一方，複数の海事事例より GPS への攻撃が報告され，GPS の脆弱性が明らかにされている．しかし，航海システムを含む船舶におけるサイバーセキュリティ対策は非常に遅れており，多くの海事機関が様々な対策を探っているが，従来のサイバー攻撃対策が中心であり，船舶特有の対策は少ない．

本論文は，船舶に与える GPS 信号の重要性を提示するために，先ず，GPS と GPS ベースの航海システムの関係を調査する．次に，GPS ベースの航海システムに対するジャミングやスプーフィング等の電波攻撃の蓋然性とセキュリティ対策を調査する．併せて，GPS への攻撃による航海システムと船舶への影響，船舶特有の外洋・近海に分けた対策を整理し，GPS に依存しない手法として，GPS と既存の航海システムの適用手順を示したレスポンスチャートを提案する．そして，GPS スプーフィング攻撃に対する航海士の対応と提案手法の類似性について，操船シミュレータ装置を用いて検証し，新たな問題点を抽出すると共に，今後の船舶運航に必要な対策を導く．

Abstract

Navigation systems such as AIS and ECDIS are indispensable for ship operations, and many of them relies heavily satellite systems such as GPS to obtain the acquisition of location information.

On the other hand, several maritime cases have reported attacks on GPS, and the vulnerability of GPS has been revealed. However, cyber security measures for ships, including navigation systems, have been very slow and many maritime organizations are exploring various countermeasures, but most of them are focused on conventional cyber-attack countermeasures and few are specific to ships.

This paper first investigates the relationship between GPS and GPS-based navigation systems in order to present the importance of GPS signals to ships. Next, the probability of radio frequency attacks such as jamming and spoofing against GPS-based navigation systems and security measures are investigated. We also examine the impact of GPS attacks on navigation systems and vessels, and the ship-specific countermeasures for open-sea and near-sea vessels, and propose a response chart showing the procedures for applying GPS and existing navigation systems as a GPS-independent method. Then, the similarity between the navigator's response to a GPS spoofing attack and the proposed method is verified using a ship-handling simulator device to identify new problems and to derive countermeasures necessary for future ship operations.

目次

図目次

表目次

第 1 章

序論

1.1 研究背景

海事業界では，衛星回線などの海上ブロードバンド通信や ICT 技術の発展に伴い，サイバー攻撃が船舶の航行安全の侵害や経済的被害等の様々なリスクが懸念されている．船舶においては，自動船舶識別システム (AIS) や電子海図情報表示システム (ECDIS) 等の航海計器の普及，センサ，IoT，AI，ビッグデータ処理の急速な進歩など技術的発展している．大型な船舶が，これまでになく少ない乗組員で運航される傾向にあり，乗組員の需給が逼迫し，作業負担の軽減・効率化のために，各国で自動運航船の技術の開発・実用化の研究プロジェクトが進められている．日本では，国土交通省によって自動運航船の実現に向けて段階的に目指す予定であることが示されている．従来船において，各機器，システムが独立していところ衛星回線の高速化が進んだことで，一部システムが結合され，陸上とのデータ通信が可能となった．

海事産業は比較的小規模な産業であり，例えば，総トン数 100 以上の推進力のある海上商船が約 98,000 隻，国際的に運航されている [1]．このため，この業界が体系的な分析を行ったり，他から学んだりすることには限界があり，サイバーセキュリティ対策を改善することが難しい．船舶は，様々な ICT が搭載された複雑な「帆船村」である．その範囲は，事務システムから，生命維持システムやエンジンの自動化，航海システムまで多岐にわたる．船舶の寿命は通常 25 〜 35 年で，ソフトウェアのアップグレードは個々の機器ごとに異なる時間間隔で行われる．つまり，ほとんどの船舶は，一般的な IT（情報技術) 用と OT（運航技術) 用の機器が混在しており，複雑であることからメンテナンスが非常に難しい．船舶は国際的な規制下にあるが，その規制は経済的な公平性を確保するための最低限の技術的要件に重点を置く傾向にあり，国際競争が激しく，コストに非常に敏感な市場である海事業界で関係者の多くがサイバーセキュリティに必要な優先順位を与えていない． 海事業界におけるサイバーセキュリティに関するインシデントは，一般的なサイバーセキュリティインシデントと比べると公表されている情報は非常に少ない．これは海事業界において公表するインセンティブがないためとされている．また，業界自身による報告バイアスが存在するためとも言われている．それでも昨今のサイバーセキュリティへの脅威となる傾向にあることから隠蔽するには大きすぎるものは報告される件数も増えつつある．また，年及び攻撃場所に関連するインシデントの数は，明

確な傾向を明らかにするための統計的有意性を持っていない．したがって，結果の定性的な解釈をせざるを得ないとされる [2].

過去 14 年間（2010 年 ～ 2024 年) に発生したもので，船舶へ影響与えたサイバーインシデントは，主に電波妨害とマルウェア (特にランサムウェア) 感染の 2 種類が占めている (**表 1.1**) .

船舶の IT システムがマルウェアに襲われたインシデントはいくつかあるが，攻撃ベクトルは標的型というよりは偶然に起きた事例が多い．典型的な攻撃ベクトルは電子メールの添付ファイルやリンクであり，船舶のサーバーやクライアントが使い物にならなくなってった事例多い．データはすべて消去されるため，残されたフォレンジックできる証拠は限られていることから調査に難航する．

OT システムは通常，他のシステムから分離されているため，露見することは少ない．それでも，OT システムに対するインシデントの例は起こっており，その結果は重大なものとなっている．攻撃の例は，感染した USB メモリや，意図せず誤ったネットワークに接続されたコンピュータを介してシステムに侵入されている．攻撃対象となるシステムの例としては，ECDIS や推進制御システム等があり，海図の更新やシステムのアップデート作業等で起きているようである．

陸上施設や海上施設の通信システムに対する攻撃の例もいくつかある．船舶の通信への影響は少ないが，船内には多くの異なる必要な通信システムがあり，潜在的な被害者であることに変わりはない．これらのインシデントは，ハッキングやランサムウェアによる可用性の損失をもたらす傾向があることを示している．

船舶の位置情報の取得は，主に GPS (Global Positioning System：全地球測位システム) [7] の信号を利用している．船舶が航行目的で利用する GPS 信号であるため，その GPS 信号への攻撃は「妨害」，または「なりすまし」に関連する電波妨害が多い．この種の脅威は通常，黒海のような地政学的紛争地域で顕在化する傾向にある．

船舶の運用に用いるシステムは，IT と OT の統合が進んでいる．船舶における OT は，機械的サブシステム，または電気的サブシステムに関連する機器で，船内作業の自動化によるコストの削減と乗組員による危険な作業の低減を可能にしている．一方，船舶における IT は，船舶の航行計画，航行制御，監視等の支援を提供する．大きな旅客船やタンカー等の国際航海を行う商業船舶は，多国間条約により様々な電子機器の搭載を義務付けられる対象となっている [8]．IMO (International Maritime Organization：国際海事機関) が推進する e-Navigation[9] などの規定や取り組みにより，複数のシステムが複雑に統合した大幅な船上システムのデジタル化に繋がっている．中でも統合航法システム (INS：Integrated Navigation System) は，このデジタル化の中核をなすものである．様々な航海システムからの情報を収集，機能を統合することで，INS は航海士を支援し，船舶の全体的な状況認識の向上に貢献している [7].

一方で，船舶の運航において航海術が，操船術と並んで，航海士の基本技術のひとつである．かつては，天文航法という技術が船舶や航空機の航法の要だったが，現在では，その多くが電波航法に取って代わられていた．電波航法については，技術の発展によりロラン等の地上

表 1.1: 船舶へ影響与えたサイバーインシデント (2010 〜 2024 年)[2]

年	攻撃	概要
2016	電波妨害	韓国にて，280 隻の船舶が航海システムに問題を起こし，港に引き返えさなければならなかった．北朝鮮が原因とされているが，証拠は乏しい [3].
2017	電波妨害	ノヴォロシースク近郊の黒海で，少なくとも 20 隻の船舶の位置情報が実際の位置から約 32km 離れた位置を示していた．これらの観測は GPS スプーフィングによるものと思われる．[3][4].
2018〜2019	電波妨害	ノルウェー北部で約 2 年間で GPS 妨害が複数回観測された．ある程度の影響はあったが，幸いにも深刻な被害は回避された [1].
2019	電波妨害	黒海で船舶が GPS スプーフィングにさらされる．船は海上にあるが，船舶の航海システムの位置情報は多くの船が陸上にあると示していた．この現象は 3 日間に 4 回発生し，最大発生時間は約 30 分だったとされる [2].
2019	マルウェア	ニューヨークに向かう大型船が，船内の制御システム・ネットワークがマルウェアに感染し，機能が制限された [5].
2019	マルウェア	フィンランドのナーンタリ港近くのタンカーの管理サーバーがランサムウェアに感染し，バックアップデータも消去された．リモート・デスクトップ・プロトコル (RDP)，USB デバイス，電子メールの添付ファイル等が攻撃経路として特定されている．また，同船舶はこの 4 ヶ月後に，同じ港の近くで再感染している [2].
2019	マルウェア	同じ所有者の 2 隻の船舶が電子メールに添付された Word ファイルによりランサムウェア「Hermes 2.1」に感染した．管理ネットワーク上の複数のワークステーションが影響を受けた [2].
2020	マルウェア	英国 Tynemouth 近郊に停泊していた船舶の船舶サーバーと複数のクライアント PC がランサムウェア「Ryuk」に感染した．全データが暗号化され，システムが使用不可に陥った．完全再インストールによりシステムを復元した [2].
2020	マルウェア	アメリカ船籍の船舶 3 隻の管理システムにランサムウェア「Sodinokibi」が感染した [2].
2023〜2024	電波妨害	北欧やバルト海沿岸諸国を標的としたロシアによるものと思われる GPS の電波妨害やスプーフィングが 6 件以上発生．ロシアへの経済的，戦略的な影響を与えるために，新規衛星に対する新しい周波数割り当て拒否等の対応措置を取るべきだとしている [6].

ベースのシステムから GPS のような衛星ベースのシステム，GPS の測位を補正する DGPS (Differential Global Positioning Systems) のような混合システムなど様々なシステムが存在する．なお，日本における DGPS については，GPS の精度向上, QZSS (みちびき) 等の補正システムの運用開始が見込まれたことにより 2019 年に廃止されている [10].

その上で，SOLAS (The International Convention for the Safety of Life at Sea：海上における人命の安全のための国際条約) で規定された船舶には，乗組員の支援のために搭載が義務化されている ECDIS 等の航海システムなど，船舶特有のシステムを搭載している．

そして, 2021 年以降, IMO は, SOLAS における国際安全コード (ISM コード：International Safety Management Code) に基づき, すべての船舶の船主・運航者の安全管理システム (SMS：Safety Management System) にサイバーリスク分析と船舶及び船舶システムをサイバー攻撃から保護する方法を含めることを義務付けている [11]．IACS (International Association of Classification Societies：国際船級協会連合) から，船舶のサイバーレジリエンスに関する最低限の要件として，NIST CyberSecurity Framework を適用した E26 (船舶のサイバーレジリエンス) [12] と 船上のシステム及び機器のサイバーレジリエンスに関する統一規則として，IEC62443 を適用した E27 (船上のシステム及び機器のサイバーレジリエンス) [13] の 2 つの UR(Unified Requirement：統一規則) が発行された．2024 年 7 月以降の建造契約の船舶に適用される予定である．しかし，電波妨害へのセキュリティ対策は，あまり多くは記載されていない.

そして，昨今，乗組員の確保が困難になりつつあることから，更なる船舶運航の作業低減のため，自立的な判断と操作機能の付加を目的とした自動運行船の実現への計画が進められている [14].

1.2　研究目的

本論文の研究目的は GPS 及び航海システムの脆弱性，GPS への攻撃とその影響，現在の防御のためのセキュリティ対策の調査を行い，新たな航海システムのセキュリティ対策の課題抽出のため，GPS に依存しない手法の提案し，その類似性の検証を行う.

1.3　研究成果

本研究の貢献として，以下のとおりである.

- GPS に対する攻撃による航海システムと船舶への影響，船舶特有の外洋，近海に分けた対策の整理
- GPS と既存の航海システムの適用手順を示したレスポンスチャートの提案
- 広島商船高専の操船シミュレータ装置を利用した GPS スプーフィング攻撃とレスポンスチャートの類似性検証，及び新たな問題点抽出検証

なお，本論文は，情報処理学会の”コンピュータセキュリティシンポジウム 2023”[15] 及び

電子情報通信学会”暗号と情報セキュリティシンポジウム 2024”[16] で発表している．

1.4　本論文の構成

本論文の構成は，以下のとおりである．

第 2 章では，船舶の位置情報取得をするために，運航者 (航海士) のツールである既存の航海システム操船術としてと船舶を航行する上で必須でなる航海術の既存の手法及び支援システムについて述べる．第 3 章では，GPS の基本技術の特徴を述べる．第 4 章では，GPS への攻撃として，主に電波妨害における攻撃の特徴と対策について，関連研究を述べる．第 5 章では，GPS への攻撃を受けた場合の対応として，既存の航海システムにおける適用手順を示したレスポンスチャートの提案を行う．第 6 章では，GPS スプーフィング攻撃への対応について，本研究の提案するレスポンスチャートの類似性の確認のため，操船シミュレーション装置を利用して検証する．最後に，第 7 章で本研究のまとめと今後解決すべき課題について述べる．

第 2 章

技術背景

本章では船舶の技術背景である操船術と航海術について解説する．船舶には操船を補助するために航海システムが搭載されている．航海システムは複数の機器で構成されている．

2.1　操船術の技術背景

操船術としては，以下の技術について述べる．

- AIS (Automatic Identificaion System：自動船舶識別システム)
- 船舶レーダー (Marine Radar)
- ECDIS (Electronic Chart Display and Information System: 電子海図表示情報システム)

2.1.1　AIS

AIS (Automatic Identification System：自動船舶識別システム) とは，VHF 帯無線を利用し，船舶間，または船陸間で情報の送受信を行い，船舶の航行安全と効率的な運航の支援，船舶交通業務運用の改善のためのシステムである．全ての旅客船，国際航海に従事する総トン数 300 トン以上の船舶及び国際航海に従事しない総トン数 500 トン以上の船舶に対して搭載が義務化されている．船舶の船名，識別符号，船の種類等の静的情報，船の位置，針路，速力，航行の状態等の動的情報，目的地，到着予定時刻等の航海情報等の情報を交換する．なお，動的情報は，船舶を表すターゲットシンボルとベクトルを船舶レーダーや ECDIS のプロッタ画面に表示させることで，自船と他船の船速と針路の把握が容易にしている [17]．また，AIS には，GPS と同様の脆弱性とリスクを持っている [18][19].

2.1.2　船舶レーダー

RADAR (RAdio Detection And Ranging) は，電波を使って周囲の物体を検出するシステムである．レーダーシステム全体はさまざまな装置に依存するが，アンテナユニットと表示装

置の構成，すなわち PPI (Plan Position Indicator) の 2 つの主要なものだけを考えた場合，アンテナは垂直軸を中心に 360 度回転し，電波を放射して目標からの反射波を受信する．

船舶に搭載される船舶レーダー (Marine Radar) は，他船や航路標識，陸岸などの映像を検出し，当該映像の方位・距離，またはそれらの時間変化の情報などから，乗組員の状況認識を形成し，船舶遭遇状況や避航動作 (衝突や乗揚げの回避) の判断や位置測定など重要な役割を果たしている [20]．ECDIS や AIS が登場するまでは，船舶の第二の目として活用されてきた．船舶レーダーは，ARPA (Automatic Radar Plotting Aid) により，他船の軌跡を自動的に検出することができる [21].

船舶レーダーシステムと INS のコンポーネント間の統合は，航法ネットワークによってサポートされ，2 つの標準ネットワークプロトコル「NMEA 0183」と「ASTERIX CAT-240」[22] である．前者はすべての機器間の相互接続を可能にし，後者は船舶レーダーアンテナとディスプレイ間のビデオデータ伝送を可能にする．船舶レーダーに利用される周波数は 2 種類で，X バンド (9 GHz 帯) と S バンド (3 GHz 帯) である．X バンドレーダーは，S バンドレーダーに比べて，比較的小型のアンテナで大きな利得や鋭い指向性が得られる．一方，S バンドレーダーは，X バンドレーダーに比べてアンテナが大型になるが，霧，雨，海面反射の影響下でも物標検出能力が維持されるという特徴を持つ．大型船のように 2 台のレーダーを装備する場合には，X バンドと S バンドを 1 台ずつ装備することが一般的である．

船舶レーダーアンテナにはメーカーによって異なる仕様があり，回転速度，ベアリングやレンジに関連する分解能などがある．回転速度は，モーターがアンテナを回転させる速度を指定する．方位分解能（角度分解能) は，同じ距離にあるターゲットと近くにあるターゲットを分離する能力を決定する．レンジ分解能は，同じ方向にあるが距離がわずかに異なる 2 つのターゲットを分離する能力を決定する．

アンテナの形状は，スロットアンテナが用いられ，水平ビーム幅は狭く，垂直ビーム幅は船が動揺しても物標検出ができるように大きくしている．アンテナの大きさや周波数にも依存するが，一般的に，水平ビーム幅は 1 〜 2° 程度，垂直ビーム幅は 20 〜 30° 程度である．また，海面反射の影響を軽減するために水平偏波が用いられる．

2.1.3　ECDIS

ECDIS (Electronic Chart Display and Information System：電子海図表示情報システム) [23] は，ENC (Electronic Navigational Chart：電子航海海図) を最下層のレイヤーとして船舶レーダーや GPS を含む様々なセンサ機器のデータを集約，各データをレイヤーごとに重ねて表示させ，航海士の支援してくれる紙海図と同等に取り扱うシステムである．

SOLAS の船舶に搭載が義務化されており，船に 2 台搭載した場合，紙海図の搭載が免除される．

ECDIS はバックアップの構成 (配置) ，基礎となるオペレーティングシステムの更新と安全なセットアップに起因する弱点に対して致命的な脆弱性があることが示され，加えて，サイバー脅威のリスクレベルが高いと判断されている [24][25].

図 2.1，**図 2.2** に本研究で取り扱う航海システムである AIS，船舶レーダー及び ECDIS の構成を示す．船舶に搭載されているセンサ群は，概ね GPS 衛星，他の船舶，陸上通信局からの無線信号を受信すると各データを NMEA 0183 規格の通信プロトコルにより各システムへ一方向で送信される．NMEA 0183 規格は，GPS 受信機や航海システムの通信規格として米国海洋電子機器協会 (National Marine Electronics Association) により規定・管理されていたものであり，IEC61162-1 及び IEC61162-2 として国際標準化された．7 ビット ASCII による非同期シリアル通信が用いられ，データ送信側と受信側の機器はそれぞれトーカとリスナと呼ばれ，単一のトーカから単一あるいは複数のリスナへデータが送信される．

ECDIS に表示される海図である ENC は， データを迅速に表示できるような効率的なデータ構造にするため，ほとんどの ECDIS は S-57 による各 ENC データセットの規格である SENC (System ENC) によって表示される．SENC は，ECDIS 内部の機械言語のフォーマットに変換する．また，SENC フォーマットは，各 ECDIS メーカー毎に異なる．

ECDIS の機能要件は以下の通りである．

- SENC 情報のすべてを表示できる．
- 安全等深線，安全水深を選択でき，強調表示できる．
- ENC の更新ができ，正しく SENC にロードされていることを確かめる手段を持つ．
- ECDIS にレーダー情報，RP (Radar Plotter) 情報を表示する場合，海図とレーダー映像，RP 情報は縮尺，向き，投影法が合致する
- ECDIS に真方位表示を備えている．

また，ECDIS に必須である ENC のデータ更新は，インターネットを介する場合，またはメール等によりデータをダウンロードする場合に手動で USB メモリ，または DVD 等の外部記録媒体を介して行われるため，エアギャップ間のマルウェア等の感染リスクが内在する．

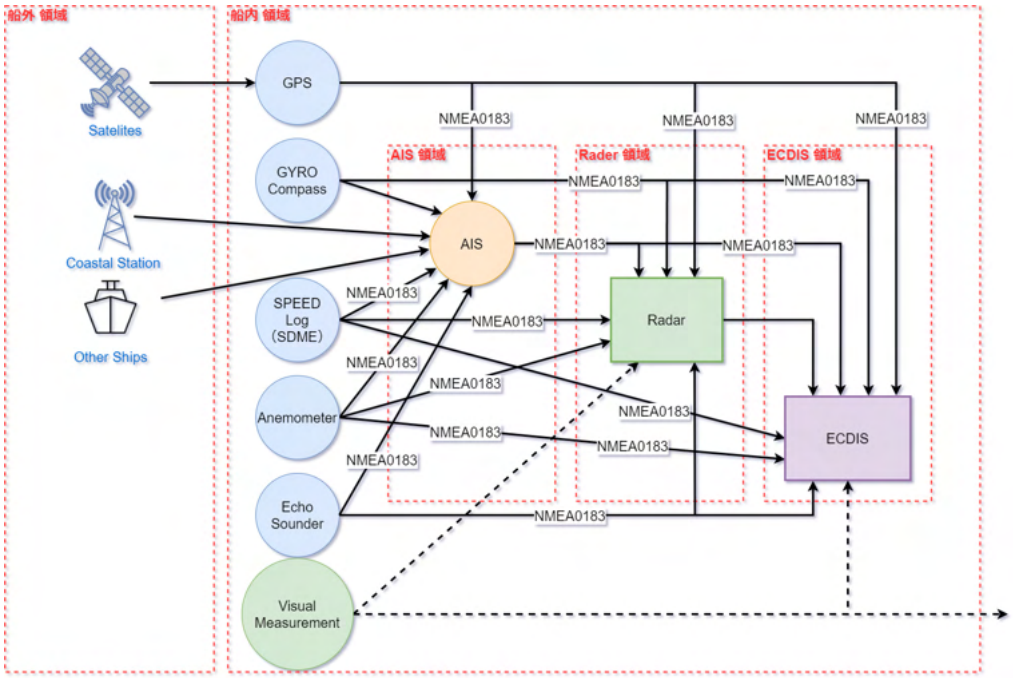


図 2.1: 航海システムの構成

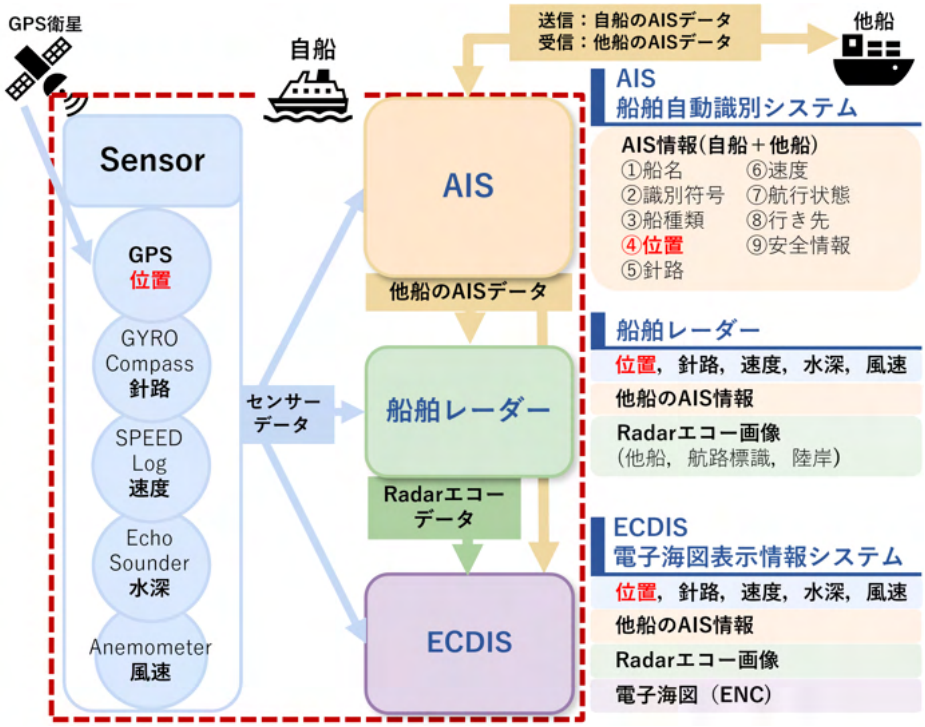


図 2.2: 航海システム (AIS，船舶レーダー，ECDIS)

2.2　航海術の技術背景

船舶の移動において，地球表面上に描かれる線分には，次のような線分がある．

- 航程線：船舶が針路一定で航走した場合に描かれる線分で各地の子午線との交角が一定である
- 大圏：球表面にある 2 地点を最短の距離となるように結ぶ線分で大洋を横断する場合に使われる．

なお，真子午線 (真南北線) を基準にした時，それと船の航跡の交角を真針路 (True Course) といい，船首と船尾を通る線 (船首尾線) との交角を視針路 (Apparent Course) という．また，真子午線と測者及び物標を通る大圏との交角を真方位 (True Bearing) といい，コンパスの南北線と測者及び物標を通る大圏との交角をコンパス方位という．

船舶の航法 (Navigation) とは，船舶をある地点から目的の地点まで導くための方法である．船舶が通過する航路は，自動車が走る道路のように明確な道筋がある訳ではない．また，風や波浪等の外力の影響を受けることにより船舶は航路上を正確に辿ることはできず，航路から外れることとなる．よって，船舶を目的の地点に導くには，周期的に正確な位置を求め，針路と速力を修正しなければならない．

船舶の航法には大きく分けて慣性航法，地文航法，天文航法，電波航法の 4 つに分かれる．最初に開発された航法は，著名な物標等の地物を目印にして利用する地文航法である．その後，外洋を航行するために，天体を利用する天文航法が開発された．また，船の針路を取得するために慣性航法が存在する．

2.2.1　慣性航法

航法のシステムは古い歴史の中で，多方面の技術開発を背景として発展してきた．その過程の中で，慣性航法システム (INS：Inertial Navigation Systems) は，船舶の針路を示す 慣性航法 (Inertial Navigation) の最も重要なシステムである．

慣性航法システムの仕組みは，加速度計とジャイロスコープの慣性センサ (IMU：Inertial Measurement Unit) を用いて，加速度と方向を測定することで，船首の向いている方位を取得できる．そして，それらを積分することで速度と距離を求めることが可能となる [26]．また，起点の位置を入力しておくことで，移動した距離と方向から相対的に現在の位置を算出することが可能である [27]．よって，自船の位置を相対的に算出するため，起点や方位が必須となる．

慣性航法システムは，外部から電波信号に依存しないため，天候や妨害などの影響を受けにくいが，センサーからの測定値を積分することで相対的に自船の位置を算出することから，長時間，長距離にわたるとジャイロコンパスの誤差や積分誤差が累積されていくため精度が低下する．

2.2.2　地文航法

地文航法 (Terrestrial Navigation) とは，海図に記載されている顕著な物標 (山頂，岬の先端，灯台等の地物) を利用して，船位 (船舶の位置) を確認しながら，目的の地点まで導く方法である．船舶は地球表面の 2 次元空間上にあるため，位置を確定するには物標の位置と船舶との位置関係の方位，距離，重視 (2 つの物標が同一方向にて重なって見える) の要素を 2 つ以上求める必要がある [28].

地文航法には，船位の導出に多種多様な個別の航法がある．その中でも沿岸を航行中に最も多く用いられ，精度の良い船位が得られる測位は，クロスベアリング (Cross Bearing：交差方位法) と呼ばれる方法である．クロスベアリングは，複数の物標 (2 物標以上) を選び，それぞれの物標の方位を測定して，その線分である位置の線 (LOP：Line Of Position) の交差点により船位を求めることで位置情報を取得する (**図 2.3**)．但し, 3 物標の方位を測定する場合は，測定に生じた誤差が重なると 3 物標からの位置の線が一点で交わらず，誤差三角形 (Cocked Hat) が生じてしまう (**図 2.4**)．誤差三角形をできる限り小さくするためには，位置の線の交角に留意して，位置が正確で，距離が近い顕著な物標を選定し，方位変化が早い物標から速やかに方位測定することが求められる．

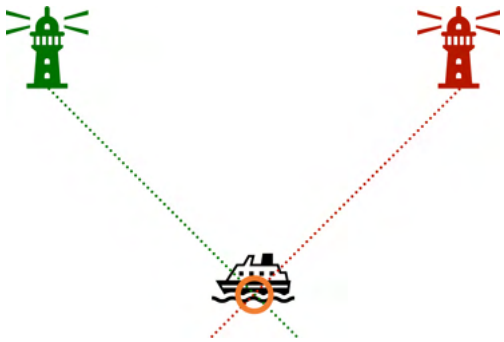


図 2.3: クロスベアリングによる位置の取得 [28]

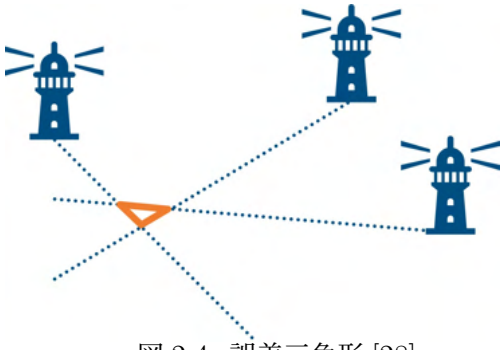


図 2.4: 誤差三角形 [28]

2.2.3　天文航法

天文航法 (Celestial Navigation) とは，天体を利用して，船位を確認しながら，目的の地点まで導く方法である [29]．天文航法で行う天測では実在する「地球」と「天球 (Celestial Sphere) 」という仮想の球の 2 つの球を便宜的に使い分ける．天球は，地球を中心に半径無限大とする先に天球の表面を想定し，その表面に天体が配置されていると考える，そして，天球上の天体の位置は固定で考える．地球は天球の中心で回転するため，天球上における太陽の位置は，見掛け上移動することとなり，移動した軌跡を黄道と呼ぶ．また，黄道と天球上の赤道 (Equator) が交差する 2 点を，それぞれ春分点 (Vernal Equinox)，秋分点 (Autumnal Equinox) と呼ぶ．

天球上における天体の位置は，赤緯 (Declination：赤道からの角度) と赤経 (Right Ascension：春分点からの角度) で表す．観測する時刻で，対象とする天体が船舶から見てどこに位置するかは，地球上の緯度と天球上の赤緯との差である地方時角 (Local hour angle) で表すことができる．春分点がその地の子午線を通過してからの経過した時間 (経度時) は恒星時 (Sidereal Time) であり，我々が通常使用している時間は，赤道上を等速で進むとする仮想の太陽 (平均太陽) を基準とした時間 (Mean Solar Time：平時) である．

そして，平均太陽の赤経 (Right Ascension of Mean Sun) と各天体の赤経との関係は「天測歴 (日本版)」，または「The Nautical Almanac (英国版)」 から知ることができる (天測歴は既に廃止されている [30])．観測時の平時が分かれば，その時点の天体の地球上における位置 (赤緯，地方時角) がわかる．天体と船舶の関係で観測できるのは，天体の方位と高度であるため，観測した高度を補正することで真高度 (True Altitude) を求める必要がある．その一方で，推測位置 (Dead Reckoning Position) を基に天体の高度を計算（計算高度：Calculated Altitude) することができ，観測した位置が推測位置と異なるため，観測位置と推測位置の緯度の差，経度の差を 2 つ以上の天体を観測から作図・計算によって求めることができる．

船舶での天測の流れは，「準備」，「高度の測定」，「位置の決定」の 3 つのフェーズで行い，以下のとおりとなる [29](図 **2.5**)．

(1)　準備

1. 世界時の把握
   天体の計算高度を求めるためには，天体の位置が必要である．天体の位置は The Nautical Almanac に記されている．世界時 (UTC) の時刻を基に The Nautical Almanac から対象とする天体の位置を検索するため，天測時点の世界時を把握しなければならない．世界時を把握しておくために，船舶においてはクロノメーター等の高精度の船用基準時計が必要となる．ただし，時計に誤差 (クロノメーター・エラー等) が生じるため，把握しておく必要がある．
2. 六分儀の器差の把握
   六分儀の器差 (インデックス・エラー) が高度計算に影響するため，把握しておく

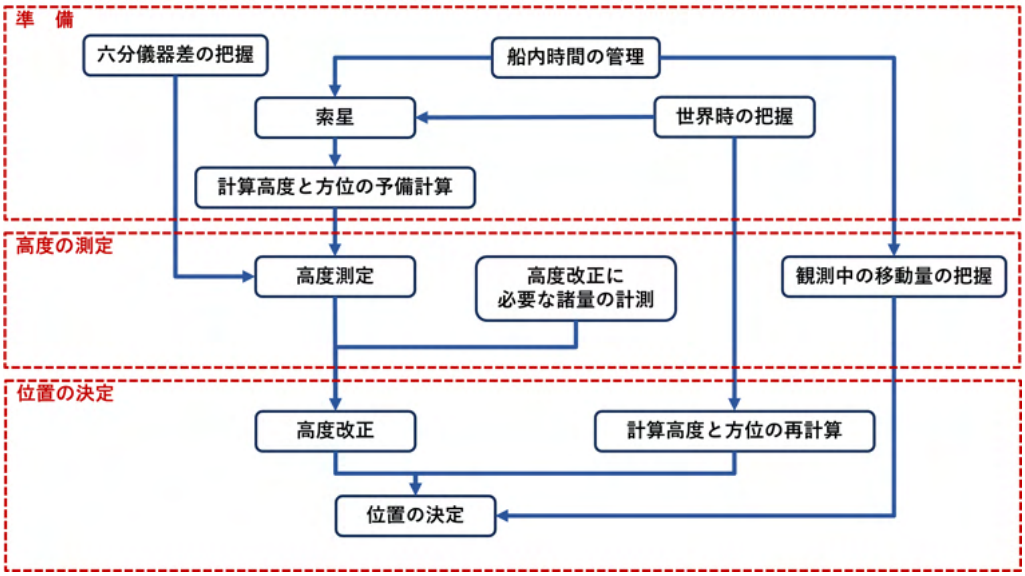


図 2.5: 天文航法における天測全体の流れ [29]

必要がある．

3. 船内時間の管理

六分儀を用いる天体の高度の測定には，水平線を視認できることが条件である．観測時期の選定には，水平線を視認できる昼間，日出没の時刻や薄明の時間帯を考慮する必要がある．

4. 索星

観測する天体を特定する必要がある．対象とする天体は前述のとおり，太陽，恒星，惑星，月が候補となる．しかし，観測する時点での天頂から真水平までの 90° の範囲内にある天体が観測の対象となる．また，位置の線同士の交差角を考慮しながら，天体の等級や光線の屈折の程度を総合的に勘案する必要がある．

5. 計算高度と方位の予備計算

上記 1 〜 4 から観測する時期と推測位置が定まれば，あらかじめ各天体の方位と計算高度を求めることが可能である．観測時は，方位と本船の針路を勘案して，索星した天体が本船のどちら側に見えるのかを確認しておくことが重要である．

(2)　高度の測定

1. 高度改正に必要な諸量の計測

測定した高度の改正 (高度改正) をより適切に行うため，大気の状態 (気圧，気温と海水温度) 観測する必要がある．眼高も高度改正に必要な要素のため，観測する甲板上での目線の高さを確認しておくことが必須である．

2. 高度測定

六分儀の望遠鏡内において天体と水平線が一線になった時の示度 (六分儀高度) と

UTC を記録する．

3. **観測中の移動量の把握**
   薄明時の観測では，複数の天体についてそれぞれの六分儀高度と UTC を得る．本船は僅かに移動しているため，各位置の線には微調整が必要となる．観測時の針路と速力も確認しておく必要がある．

(3)　**位置の決定**

1. **計算高度の再計算**
   高度を測定したときの船内使用時と UTC から，改めて推測位置と天体の位置を求め，これらを元に計算高度と方位を再計算する．予備計算した計算高度は，実際に測定した時刻とずれがある．時刻のずれが大きいほど，推測位置もずれるため，修正差が大きくなる．修正差が大きくなると，推測位置から離れたところに位置の線の交点が現れる．交点と推測位置の間が離れるほど，直線で近似する際の誤差の影響が現れる．これを避けるための再計算である．
2. **高度改正**
   高度を測定した際の六分儀の読み取り値が六分儀高度である．これに器差 (I.E.) を加減して，観測高度 (Observed Altitude) を得る．この値に種々の高度改正を加えて真高度を得る．
3. **位置の決定**
   真高度から計算高度を減じて，修正差を得る．修正差と方位から位置の線を特定し，作図あるいは計算により，真の位置として緯度と経度を確定する．

天文航法は，特有の計測方法から自動化が非常に難しい．そこで，自動運行船においては，人間の視界 (目視) に代わる方法として，カメラの撮影により得られた画像を利用し，機械学習により物体を識別することで可能となる．

既に天文航法の自動化の実現可能性については，深層学習と畳み込みニューラルネットワークのハイブリッドシステムにより，画像が撮影された時間と組み合わされた天体の合成画像をトレーニングするシミュレーションが検証されている [31].

2.2.4 電波航法

電波航法 (Radio Navigation) は，双曲線航法とも呼ばれ，二定点からの距離差がわかれば，その二定点を焦点とする双曲線群の一つとして位置の線が決まり，このような他の位置の線との交点として船位が決定される (**図 2.6**) .

また，その距離差の測定法として次の 2 種類がある.

(1) パルス波を用い，電波の定速性を利用して，2 地点の発信局からの電波の到達時間差を測定する (ロランシステム [32]) .

(2) 連続波を用い，2 地点の発信局からの電波の位相差を測定する (デッカシステム [33], オメガシステム [34]) .

これらの発信局は地上に設置されているが，宇宙空間に設置された場合が衛星航法であると考えれば良い．各システムの性能は**表 2.1** のとおりである.

但し, これらの発信局は既に廃局されており, 現在利用することができなくなっている [35].

表 2.1: 各電波航法システムの比較

システム名	電波	測位精度
ロランシステム [32] (Loran navigation system)	A:MF(1,750 〜 1,950kHz) C:(100kHz)	約数百 m
デッカシステム [33] (Decca navigator system)	LF(70 〜 130kHz)	約 100 m
オメガシステム [34] (Omega navigation system)	HLF(10.2 〜 13.6kHz)	約 1,000 〜 2,000 m

電波航法で最も新しいシステムは，ロランシステム (LOLAN navigation system : LOng RAnge Navigation system) である．ロランシステムは，100 kHz で作動する航法システムである．第二次世界大戦中に開発され，海上の船舶のナビゲーションで重要な役割を果たした [32].

当初，ロラン A (Loran-A) として運用され，後期型としてロラン C (Loran-C) が開発され運用された．その後，強化型の eLoran (Enhanced Long-Range Navigation) と呼ばれるシステムが研究されているが，現在の GPS の運用状況から本採用されていない．ロランシステムは，各無線局から決められた周波数信号の到達する時間の差異を利用して位置を取得する．ロラン局は，チェーンと呼ばれるグループでパルス信号を送信 (放送) し，それぞれのチェーンで特定の地域をカバーする．各チェーンは，主局 (M) と複数の従局 (W，X，Y，Z) で構成

され，従局は 8 つ，主局は 9 つのパルスを持ち，最後のパルスは主局の識別に使用される．各チェーンのパルスは，グループ反復間隔 (GRI：Group Repitition Interval) と呼ばれる一定の時間間隔で繰り返し放送される．各 GRI の繰り返し間隔は，クロスレート干渉除去のために異なるように設計されている．局のパルス間隔は 1,000 µsec で，主局の最後のパルスは 8 番目のパルスから 2,000 µsec 離れている．例えば，西海岸チェーンは GRI 9940 で，そのパルスは 0.0994 sec 毎に送信される．ロラン局は同期しており，局の送信タイミングはシステム・エリア・モニターによって制御される [36]．**図 2.7** は，ロランチェーン信号と理想的なパルスの図である [36]．ロラン C は，運用している各国同士の国際協力により無線局が連携するチェーンを形成することで，ロランシステムの位置取得を可能にしていた (**図 2.8**，**表 2.2**) [37] .

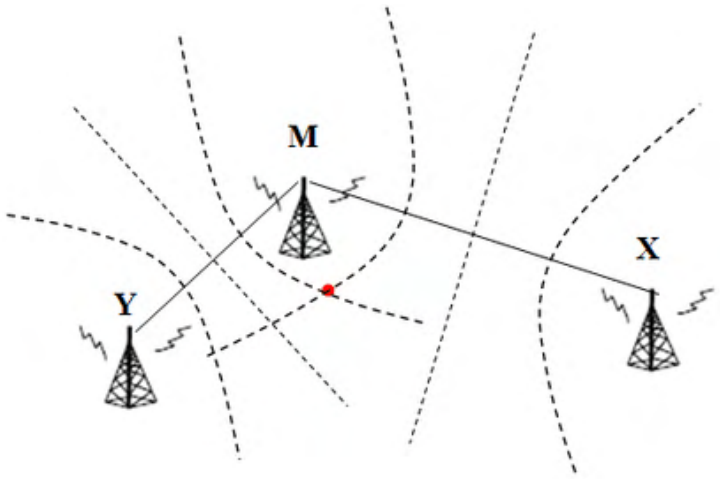


図 2.6: 双曲線による位置の取得 [36]

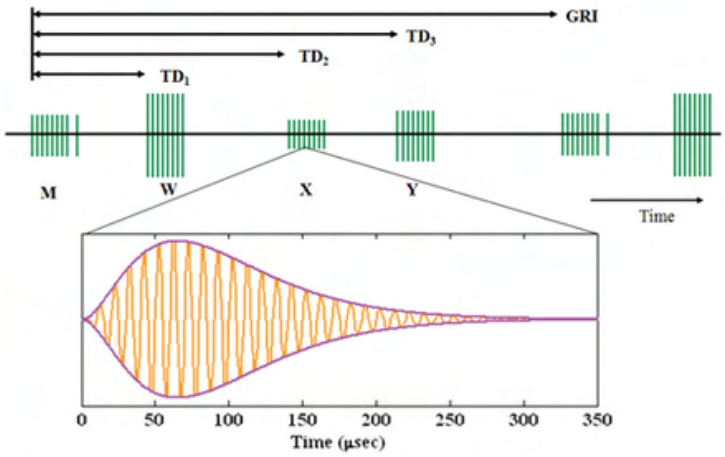
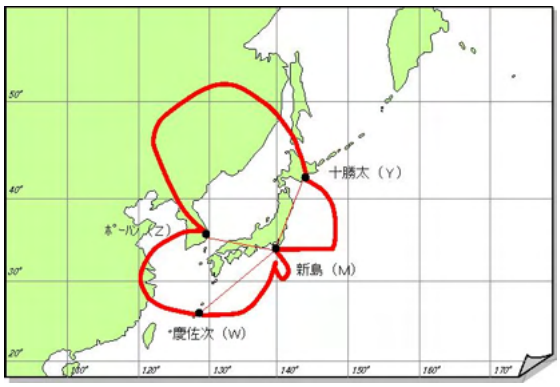
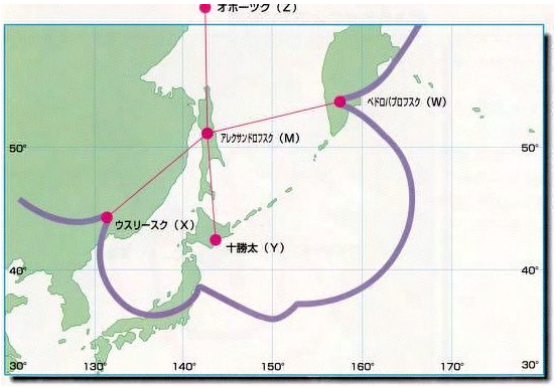


図 2.7: ロランチェーン信号と理想的なパルス [36]



(a) 北西太平洋チェーン

(b) 韓国チェーン



(c) ロシアチェーン

(d) 中国北海・中国東海・中国南海チェーン

図 2.8: ロランC国際協力チェーンの例 [37]

2.2.5　GNSS

電波航法として，GPS を含む GNSS (Global Navigation Satellite System：全地球航法衛星システム) は各国で GPS に代替えとなるシステムを開発しており，各システムの種類を**表 2.3** に記す．各システムは，互いのシステムと信号が衝突しないように異なる帯域の周波数で運用している．しかし，GNSS を利用するにはそれぞれの測位衛星の信号の周波数に対応しているか，もしくは信号を変換して受信できる受信機が必要である．

GNSS は，軌道から時間と位置を送信する衛星群であり，いくつかの衛星ネットワークが存在する．元は Navstar GPS として知られている (1) GPS，(2) 欧州連合 (EU) の Galileo，(3) ロシアの GLONASS，(4) 中国の BeiDou，(4) インドの NavIC，(5) 日本の QZSS である．

GNSS は，その性能から多くの攻撃者によって標的になる可能性がある．さらに，多くの GNSS の信号は低出力であることから，自然の太陽フレア，地球の電離層，他の無線周波数，

表 2.2: ロランC国際協力チェーンの例 [37]

チェーン名	局名	主従	送信力
北西太平洋チェーン	Niijima(Japan)	主局 (M)	1000kW
(Northwest Pacific Ocean Chain)	Tokatibuto(Japan)	従局 (Y)	1000kW
GRI:8930	Gesashi(Japan)	従局 (W)	1000kW
	Pohang(Republic of Korea)	従局 (Z)	150kW
ロシアチェーン	Alexandrovsk(Russia)	主局 (M)	700kW
(Russia Chain)	Petropavlovsk(Russia)	従局 (W)	700kW
GRI:7950	Okhotsk(Russia)	従局 (Z)	10kW
	Ussuriisk(Russia)	従局 (X)	700kW
	Tokatibuto(Japan)	従局 (Y)	600kW
韓国チェーン	Pohang(Republic of Korea)	主局 (M)	150kW
(Korean Chain)	Niijima(Japan)	従局 (Y)	1000kW
GRI:9930	Gesashi(Japan)	従局 (Z)	600kW
	Kwangju(Republic of Korea)	従局 (W)	50kW
中国北海チェーン	Rongcheng(China)	主局 (M)	1200kW
(China North Sea Chain)	Helong(China)	従局 (W)	1200kW
GRI:7430	Xuancheng(China)	従局 (W)	1200kW
中国東海チェーン	Xuancheng(China)	主局 (M)	1200kW
(China East Sea Chain)	Rongcheng(China)	従局 (Y)	1200kW
GRI:8390	Raoping(China)	従局 (X)	1200kW
中国南海チェーン	Hexina(China)	主局 (M)	1200kW
(China South Sea Chain)	Chongzuo(China)	従局 (Y)	1200kW
GRI:6780	Raoping(China)	従局 (X)	1200kW

及びスペクトル輻輳からの干渉をしばしば受けるため，重大な技術的弱点となる．

2.2.6　Galileo

Galileo[38] は，1998 年，欧州連合 (EU) が GPS システムとの完全な互換性を確保するために独立した衛星測位システムを世界中の民間利用向けに開発した．Galileo のサービスのひとつである SOL (Safety Of Life) サービスは，受信した衛星信号が Galileo によって真に送信されたものであることを保証するために，認証サービスがある．さらに，SOL サービスには完全性の監視と通知が含まれる．SOL 信号の安全な使用が仕様に従って保証されない場合，ユーザーに警告が発せられる．28 個の衛星コンステレーションと，全世界の地上管制セグメントで構成されている．2 つのシステム間の相互運用性を確保するための対策が講じられている．

2.2.7 GLONASS

GLONASS (The Global Navigation Satellite System) は，GPS に対応するロシアの衛星測位システムである [39] ．地球周回中軌道にある衛星群，地上管制セグメント，ユーザー機器から構成されている．コンステレーションは 24 基の衛星を軌道上にある．信号は，G1 (1602.00 MHz)，L2 (1246.00 MHz)，L3 (1204.704 MHz) となっており，他の GNSS の周波数帯と混信しないように周波数が割り当てられていることが特徴である．

2.2.8 Beidou

Beidou (BeiDou Navigation Satellite System) は，中国独自の衛星測位システムである [40]．BeiDou (北斗) とは，北を示す北極星を意味する．コンステレーションは軌道上に 52 基の衛星があり，他の衛星測位システムと比較して最も多い数である．衛星からの信号の周波数は 5 種類あり，B1I (1561.098 MHz) ，B1C (1575.42 MHz) ，B2a (1176.45 MHz) ，B2b(1207.14 MHz) ，B3I(1268.52 MHz) で，B1C と B2a が GPS の L1，L2 を補完している．

2.2.9 NavIC

NavIC (Navigation Indian Constellation) は，インドの国土及び周辺 (インド洋を含む) の範囲限定で GPS に対応する衛星測位システムである [41]．衛星のコンステレーションは 8 基という少ない数で運用されている．GPS と同様の周波数帯 L5 (1176.45 MHz) と 単独の周波数帯 S (2492.08 MHz) の 2 種類の衛星信号を割り当てられている．あくまで，インド周辺のみで運用可能の衛星システムであるため，GPS の代替えとして通常使用は非常に厳しい環境である．

2.2.10 QZSS

QZSS（Quasi-Zenith Satellite System) は，みちびき (準天頂衛星システム) とも呼ばれ，日本の衛星測位システムである [42]．QZSS は，GPS の補完を第一に考えられているため，GPS のすべての周波数をカバーしていることから，まさに日本版 GPS と呼べる．衛星は約 200 〜 1,000 km，約 36,000 km の準天頂軌道と静止軌道にあり，2024 年現在では，4 機体制で運用されている．このうち 3 機はアジア・オセアニア地域をカバーしている．現在は，GPS や Galileo を補完している状況にあるが，いずれは 7 機体制が確立され，日本上空に常に 4 機以上の衛星が滞空できるため，みちびき単独での持続測位が可能になると見込まれる．

また，2024 年度から衛星測位サービスにおけるスプーフィングの対策として，航法メッセージに認証情報（電子署名）を付与する「信号認証機能」が追加され，運用開始予定である [43].

表 2.3: GNSS の種類

システム名	Galileo[38]	GLONASS[39]	Beidou[40]	NavIC[41]	QZSS[42]
開発国	EU	ロシア	中国	インド	日本
衛星数	28 基	24 基	52 基	8 基	4 基
高度 (km)	約 23,000	約 19,100	約 21,800	約 24,000 (3 基) 約 250 (5 基)	約 200 〜 1,000 約 36,000
周波数 (MHz)	E1(1575.42) E5(1176.45) E6(1278.75)	G1(1602.00) L2(1246.00) L3(1204.704)	B1I(1561.098) B1C(1575.42) B2a(1176.45) B2b(1207.14) B3I(1268.52)	L5(1176.45) S(2492.08)	L1(1575.42) L2(1227.60) L5(1176.45) L6(1278.75)

第 3 章

GPS とは

3.1 GPS

GPS とは，米国政府が所有し，米国空軍が運用する人工衛星 (測位衛星) を利用した最初に身近となった衛星測位システムである [7].

3.1.1 GPS の概要

GPS を利用して測位するには，測位衛星を 4 機を用いて，位置情報 (x, y, z) を取得する．「自分」と「4 機の測位衛星」との距離をそれぞれ計算して 4 つの距離を求める．その 4 つの距離がひとつに交わる点を数学的に割り出すことで，そこが自分の位置となる．

既知の位置 $L^S \in \mathbb{R}^3$ に周回している多数の GPS 衛星送信機 S_i とし，各送信機はクロックがない同期クロックを備えているとする．正確な時刻は t^S にオフセットされ，航行信号 $s_i(t)$ を送信 (ブロードキャスト) する．その場合の信号は，速度 c で伝搬する．

座標 $L \in \mathbb{R}^3$ の位置にいる無指向性アンテナを使用する GPS 受信機 V は送信される信号を受信する．範囲内にあるすべての信号を受信する：

$$g(L,t) = \sum_i A_i s_i \left(t - \frac{|L_i^S - L|}{c} \right) + n(L, t^s) \tag{3.1}$$

ここで， A_i は L_S から L に向かう間に信号が受ける減衰であり，$|L_i^S - L|$ は L_i^S と L の空いたのユークリッド距離を表し， $n(L,t)$ はノイズである．

GPS 信号 $s_i(t)$ の特性により，受信機はこの和の各項を分離し，拡散符号のレプリカを使用することで，相対的な拡散符号の位相，衛星 ID，データ内容等を抽出することができる．そして，データと相対的な位相オフセットがあれば，受信機は各衛星の時間遅延 $|L_i^S - L|/c$ を特定することで，距離を推測することができる．

そして，3 つの既知の距離 d_i と既知の GPS 送信機の位置 L_i^S があれば，3 つの式 3.2 を L について一義的に説くことが可能である．但し，3 つの S_i がすべて線上に位置する場合を

除く.

$$d_i = |L_i^S - L| \tag{3.2}$$

本来であれば，正確で安定性の高いセシウム時計等の使用が理想的である．GPS 受信機 V は双方向のクロック同期ができないため，クロック・オフセット $(t = t^S + \delta)$ を持つことにより，式 3.1 から式 3.3 を得られる.

$$g(L, t^S) = \sum_i A_i s_i \left(t - \frac{d_i}{c} - \delta \right) + n(L, t^S) \tag{3.3}$$

一方で，擬似距離 R_i とすると，GPS 受信機は遅延 $d_i/c - \delta$ から式 3.3 を推測することができる.

$$R_i = d_i + c \cdot \delta \tag{3.4}$$

クロック・オフセット δ は，4 つ目の未知となるスカラー値を追加することで，少なくとも 4 つの GPS 送信機 S_i に対する擬似距離の測定ができれば，結果として得られる式 3.4 は L と δ の両方について解くことができ，正確な時計を必要とせずに，正確な位置と時刻の両方を取得することが可能となる.

そして，$L_i^S = (x_i^S, y_i^S, z_i^S)$ ，　$L = (x, y, z)$ ，　$\Delta = c \cdot \delta$ とすると，式 3.4 を式 3.5 に変換することができる [44][45].

$$(x - x_i^S)^2 + (y - y_i^S)^2 + (z - z_i^S)^2 = (R_i - \Delta)^2 \quad \forall S_i \tag{3.5}$$

測位衛星から送信した電波には「送信した時刻」の情報が入っているので，「送信した時刻」と「自分のところに電波が到着した時刻」との差で「電波伝搬時間」が確定する．計算上は 3 つの距離情報があれば自分の位置が特定できるが，受信機の時計にはわずかに「誤差」があるため，3 機の衛星では位置情報にズレが生じてしまう．そのわずかな誤差補正するために，最低もう 1 機の情報が必要になる.

GPS の測位方法は「単独測位」,「DGPS 測位 (ディファレンシャル GPS 測位)」,「相対測位」「RTK − GPS 測位」,「ネットワーク型 RTK − GPS 測位」があり，これらの測位方法を用いて精度の高い測位を行う.

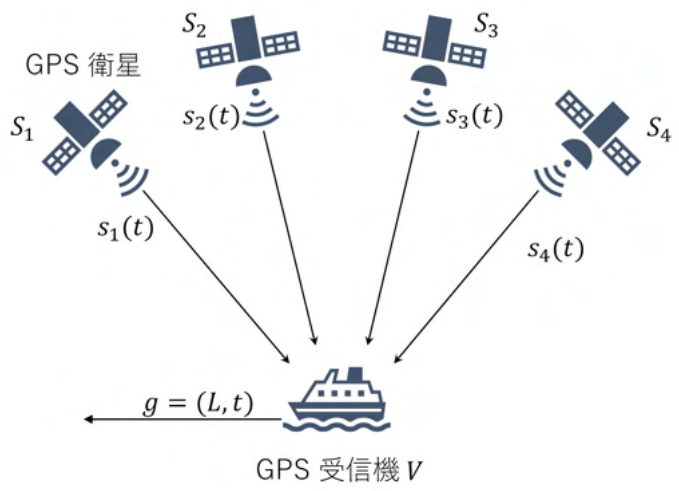


図 3.1: GPS の動作 (船舶の想定)[45]

測位手法は，大きく 2 つ「単独測位」と「相対測位」にわかれる．単独測位は全世界が測位エリアとなるが測位精度は 10 m 程度，相対測位は基準局の周辺のみとなるが高精度な測位が可能となる．

GPS は，GPS 衛星からの電波を受信することで現在位置である経緯度を知ることができる．このために，**図 3.2** のように高度 約 20,000 km の 6 つの軌道上を 31 機程度の GPS 衛星が周回 (本稼働は，24 基程度) しており，地表面に向けて常時 GPS 信号を送信している．

GPS は電波を使うため，受信機にはアンテナが必要である．アンテナが大きいほど位置精度は良く，その寸法は携帯性との兼合いといえる．また，GPS 信号を受信できないと GPS で位置を求めることはできないことから，先に述べたとおりトンネルや地下街である屋内では衛星からの障害物となるため，GPS は利用できない．屋内でも GPS 信号が入りにくいことが多いが，高感度タイプの GPS 受信機では，ある程度の位置情報を得られるよう工夫されている．

衛星とユーザ間の距離を測定し，位置を確定するには GPS 信号が少なくとも以下の 3 つの特性を備ていなければならない．

1. 電波の伝播時間から距離を測定できなければならない．
2. 3 〜 4 機以上の衛星との距離を同時に測定できなければならない．
3. 時々刻々の衛星位置をユーザが計算できなければならない．

上記の要件を満足するためには，以下の条件をそれぞれ満たさなければならない．

1. 現在受信している GPS 信号がいつ衛星から送信されたかユーザにわからなければならない．
2. 混信することなしに各衛星からの GPS 信号をユーザが受信できなければならない．
3. 衛星位置に関する情報を GPS 信号に載せて送らなければならない．

GPS のコンステレーションカバレッジは，前述で述べた陸上で運用のロランシステムを遥かに超える範囲をカバーしている [46].

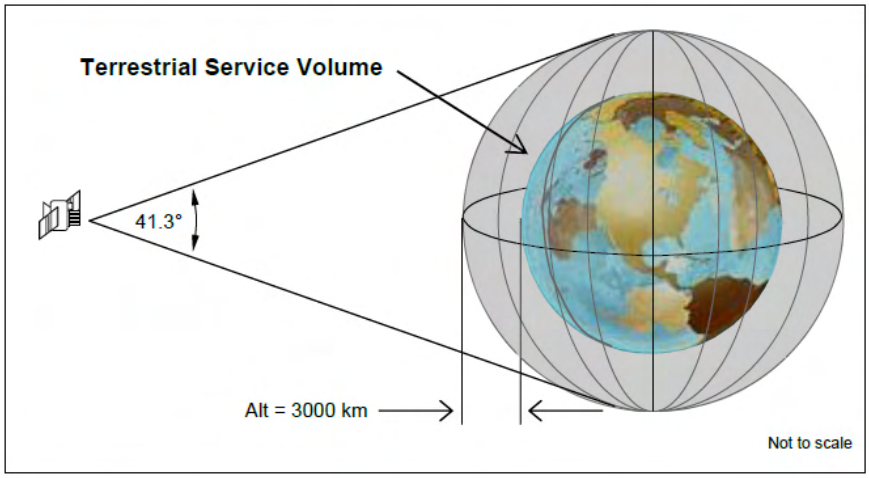


図 3.2: GPS 衛星のコンステレーションカバレッジ [46]

3.1.2　GPS 信号

GPS 信号 [47] は，PRN コード (Pseudo Random Noise Code：疑似雑音符号) と航法メッセージと呼ばれる 2 つのコードで搬送波を変調することによって作られている．PRN コードは，乱数的に「0」と「1」が現れる不規則なコードで，決まった長さで同じパターンを繰り返す．稼働初期の GPS 衛星からのデータは L1 (1575.2 MHz) と L2 (1227.6 MHz) の 2 つの周波数帯域で信号を送信している．L1 は，chip rate (PRN のデータ転送レート) 1.023 MHz/chip で 1023 chip を周期 1 ms で発生させた「 C/A コード (coarse / acquisition code) 」と chip rate 10.23 MHz/chip，周期 7 日間 で発生させた「 P(Y) コード」の 2 種類の信号が載せられている．C/A コードは GPS 衛星を識別するために民間に公表され，粗い距離測定に利用されているが，P(Y) コードは公表されずに軍事用として利用される．L2 は P(Y) コードだけが載っている．P(Y) コードは機密扱いであるが，これを受信できるシステムを入手することは可能とされる．

PRN コードの特徴は 2 つある．ひとつはコードが決まったパターンからなるので，現在受信している信号が全体のパターンの中のどの位置に当たるのかをユーザが知ることができるということである．この結果，送信側でコードの送出しのタイミングを規定しておけば，現在受信している信号がいつ衛星から送信されたかわかる．これは，コードの 1 ビットあたりの長さが短いほど精度よくわかるので， C/A コードよりも P(Y) コードの方が精度がよい．もうひとつの特徴は，PRN コードが疑似乱数であるため，変調された搬送波の信号電力が広い周波数帯域に拡散されるということである．P(Y) コードの場合は約 20 MHz の帯域に信号電力が拡散され，どちらもノイズの中に信号が埋もれてしまっている．これが，多数の GPS 衛

星が同じ周波数の電波を使っても混信しない理由で，他の衛星からの信号電力はノイズ以下なのである．このような通信方式をスペクトラム拡散通信方式と呼び，多重通信，隠匿性に優れた方式であるといわれている．受信機が特定の衛星からの GPS 信号を受信するためには，その衛星から送信される GPS 信号と同じ PRN コードをもう一度掛け合わせ，その効果を取り除くことにより可能となる．この結果，広い帯域に拡散されていた信号電力は，きわめて狭い帯域に戻され信号捕捉ができるようになる．この過程を「逆拡散」と呼ぶ．目的外の衛星からの GPS 信号も逆拡散されてしまっては混信が生じるため，PRN コードは相互相関 (異なるパターンの符号どうしの相関値) ができるだけ小さいものが選ばれている．

その後，GPS の更新過程で，L1 に L1C (L1 Civil) 信号，L2 に L2C (L2 Civil) 信号，L5 (1,176.45 MHz) と呼ばれる周波数帯域に L5 信号 [48]，更に M コードと呼ばれる軍事用の信号が L1 と L2 に追加された (**図 3.4**，**表 3.1**) [49] .

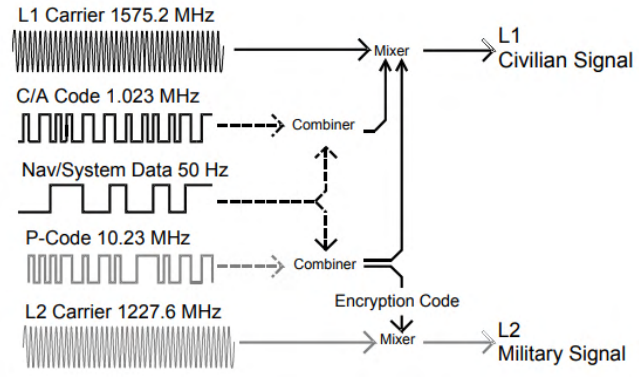


図 3.3: GPS 信号の生成例 [47]

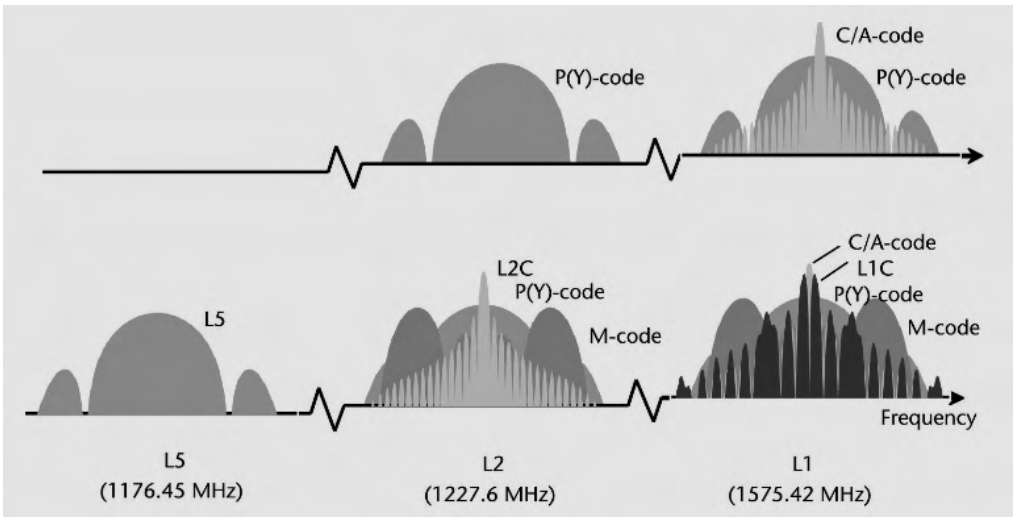


図 3.4: GPS 衛星からの信号 (旧信号 (上段) と現在の信号 (下段))[50]

また，GPS 測位精度の劣化の程度を表す数値として DOP (Dilution of Precision：精度低下率) という値がある．これは位置決定に使用する衛星群の幾何学的配置の指標であり，一般に，DOP 値が小さいほど測位精度が高いことを示している．DOP 値は GPS 衛星の位置によって左右され，上空に衛星がまんべんなく配置されていると，精度が高くなる．

送信される GPS 信号の電界強度は非常に小さい．約 30 〜 50 W で送信されるため，地球に到着する頃には 10^{-16} W となる [50] ．GPS の妨害を達成することが簡単である理由である．必要な事は，適切な周波数の信号であることである．

表 3.1: GPS 信号 (周波数帯と PRN コード)

L1 (1575.42 MHz)			L2 (1227.60 MHz)			L5 (1176.45 MHz)		
C/A	：	民間コード	L2C	：	民間コード	L5	：	民間コード
L1C	：	民間コード	P(Y)	：	軍事コード			
P(Y)	：	軍事コード	M	：	軍事コード			
M	：	軍事コード						

3.1.3 GPS 受信機の構成

GPS 受信機は，上空を周回する GPS 衛星が送信している GPS 信号をすべて受信して，GPS 衛星との間の距離を測定する．但し，障害物の陰になっている衛星からの信号は受信できないことから，実際に信号を受信できる衛星の数は限られる．GPS 受信機の方式にもよるが，最低で 3 〜 4 機以上の GPS 衛星からの信号を受信することができれば，GPS 受信機は自身の位置を計算が可能である．GPS 受信機の性能や周辺環境に大きく左右されるが，条件が良ければ，数 m 程度の精度で現在位置を求めることができる．現在では GPS 受信機の処理回路はチップ化されており，携帯電話に組み込めるレベルとなっている．

また，PRN コードの逆拡散と航法メッセージの解読を行うほか搬送波の位相追尾も行う．搬送波位相は衛星とユーザ間のドップラーシフトの積分値を表しており，デルタレンジ，及び搬送波位相と呼ばれる観測量を出力するのに使われる．受信機の構成はハードウェアの組み方によって変わるが，近年の半導体技術の進歩の結果，ほとんどがディジタル処理回路と制御用プロセッサで主要な処理を行い，アナログ部分はアンテナと中間周波数まで搬送波をダウンコンバートする回路のみとするものとなっている．ディジタル部分での処理は，PRN コードの逆拡散を行うディレイロック・ループと搬送波位相の追尾を行うコスタス・ループ，及び航法メッセージの解読を行うメッセージ解読ループからなっている．処理の順番は，ディレイロック・ループで逆拡散を行い，その後コスタス・ループで搬送波の位相同期を確立し，航法メッセージを抽出するという順が一般的である [50].

第 4 章

関連研究

本研究では，主に GPS 攻撃される可能性のある航海システムと通信回線を支えている衛星回線の機器において，関連研究を紹介する

4.1 GPS の脆弱性

4.1.1 GPS ジャミング

GPS ジャミング (GPS jamming) とは， マスキング (masking) とも呼ばれ，対象となる信号と同一周波数で同等以上の出力を持った信号を送信することにより，受信機に正規の信号とジャミング信号の区別をできなくさせる．または，正規の信号を認識できなくさせる攻撃である．ジャミングは，周波数や出力の大きさなど事前の情報収集が必要であるが，高度な技術は必要としない．**3.1.2 節**で述べたが，GPS の受信機に対する攻撃は GPS 衛星から船舶を含む地上の無線局への通信であるダウンリンクへの攻撃に絞れば良く，衛星から送信される GPS 信号の出力は，非常に小さいため，GPS への攻撃を達成することが非常に容易であり，距離にもよるが 数 W の信号で実現可能である．攻撃ツールである PPD (Personal Privacy Device) のジャマー機器に至っては，約数万円程度の安価であり，インターネット上で容易に入手できる [51].

また，攻撃は送信し続ける間のみ影響を及ぼすため，攻撃を停止すると正規の信号を元通り受信可能であり，また受信機に対して恒久的な損害を必ずしも与えるわけではない.

しかし，攻撃を受けた場合，攻撃方向の探知は可能であるが，距離の測定が困難である．また，航海システムに異変が生じた場合，それが意図的な攻撃か偶発的な障害によるもの判別が非常に困難である.

船舶に対する GPS ジャミングの関連研究として，実際の海域で GPS ジャミングの実験が行われた [52] . L1 の 2 MHz 帯域幅全体にわたる GPS ジャミングとして，既知の PRN コード (C/A コード) を地上 25 m，総電力約 2 dBW (～ 1.5 W) の低出力 (最大電力 1.58 W) で GPS ジャマーユニットからの送信による試験を実施した．GPS ジャマーユニットの電波の到達範囲の周辺海域へ攻撃対象船舶を航行させ，動的試験，静的試験を 3 日間にわたって実施

し，安全航行の様々な要素に対して GPS ジャミングの起こりうる影響が確認された (**図 4.1**, **図 4.2**)．GPS ジャミング攻撃の対象船舶は GPS 測位能力を失い，ECDIS が特に影響を受け，海上での船舶の安全航行，特に乗組員の安全航行能力に影響を及ぼされた．また，船舶の乗組員が GPS ジャミングされていることへの状況認識ができないことや代替の航行方法へ切り替えの機会を失われることにより，乗組員の安全とセキュリティに重大な影響を与える可能性があるとされた．GPS ジャミングを受けると GPS 情報を使用している自船には多数の警報が鳴り響くことによる注意散漫，夜間，または航海士と見張りのみの 2 名のみで操船される可能性がある時間帯，または船舶が高精度と高度な集中力を必要とする操縦や視界不良における作業を行っている場合によっては，さらに悪化する可能性がある．Alan[52] らは GPS ジャミングへの対策として，ロランシステムによる補完を提案している．しかし，当時は，GPS の補助手段としてロランシステムを搭載した船舶が多くあったが，昨今では各国でロランシステムのサービスの提供は廃止・縮小されているため，成り立たなくなっている [35].

図 4.1: イギリス・フランボロー・ヘッドに設置された GPS ジャマーユニット [52]

Alan[52] らの他には，GPS L1 を使用した従来の方法となる PPD ジャマー機器による攻撃の影響とドイツ航空宇宙センター (German Aerospace Center, DLR：Deutsches Zentrum für Luftund Raumfahrt) とドイツ連邦ネットワーク庁 (Federal Network Agency for Electricity, Gas, Telecommunication, Post and Railway：BNetzA) 協力の元で，Alan[52] らと同様に GNSS ジャミングテストベッドを用意し，実際の海上における GNSS ジャミングの実験が行われている [53]．Daniel [53] らは，**図 4.3** に示すように，バルト海ダルス半島の北約 10 km の位置のテストエリアにおいて，3 隻 (攻撃船 [A]，被害船 [B]，警戒船 [N]) の船舶を用意して，3 時間 (2015 年 10 月 22 日 UTC 07:00 ～ 10：00) の期間で，攻撃船は実験エリアの中心に停泊したまま，被害船は 40 m ～ 4,000 m の距離で，最高速度 8 kts で航行して試験を実施された．実験の結果から，比較的単純な仕様の PPD ジャマー機器による攻撃であったとし

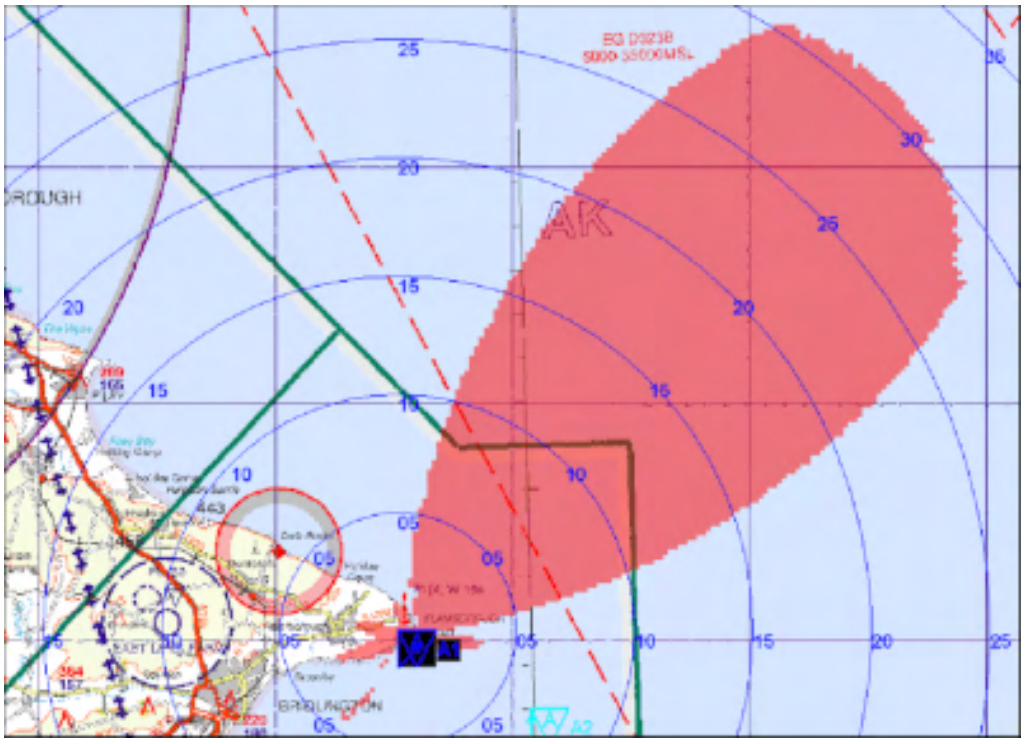


図 4.2: GPS ジャマーユニットのカバーエリア [52]

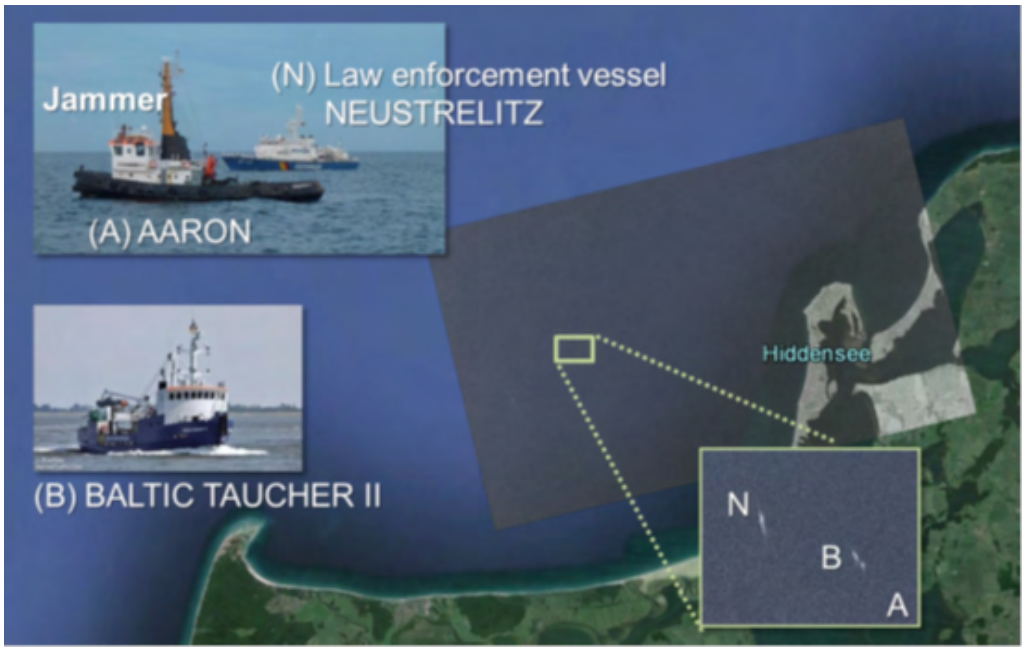


図 4.3: ダルス半島北での GNSS ジャミング実験 [53]

ても，非常に大きな領域に対して影響を与えた．一方で，攻撃源に近い場合，必ずしも GNSS に影響が出るとは限らないという結果が示されている．

4.1.2 GPS スプーフィング

GPS スプーフィング（ GPS Spoofing ）は，生成した偽信号を標的の受信機に送信することにより，欺瞞情報を与えて位置情報を混乱させるものである．GPS スプーフィングによるサイバーセキュリティインシデントは，2017 年 6 月，黒海で航行中に約 20 隻の船舶の航海システムが正常に動作していたにも係わらず，別の位置に誘導されていた事件があった．これはロシア当局による GPS スプーフィングによる GPS 信号の妨害の可能性が高いと考えられている [4]．また，この時のある船舶の GPS 受信機は，概ね同じ値の電界強度を示す GPS 衛星が複数確認されたとされており，同一の送信出力，若しくは同一の位置からの攻撃が推測される (**図 4.5**)[54]

この時の攻撃を受けた船舶は，周辺に航行している船舶に対して，同様の現象が起きているかを VHF 電話により確認したことで GPS スプーフィング攻撃の有無を判断できた．

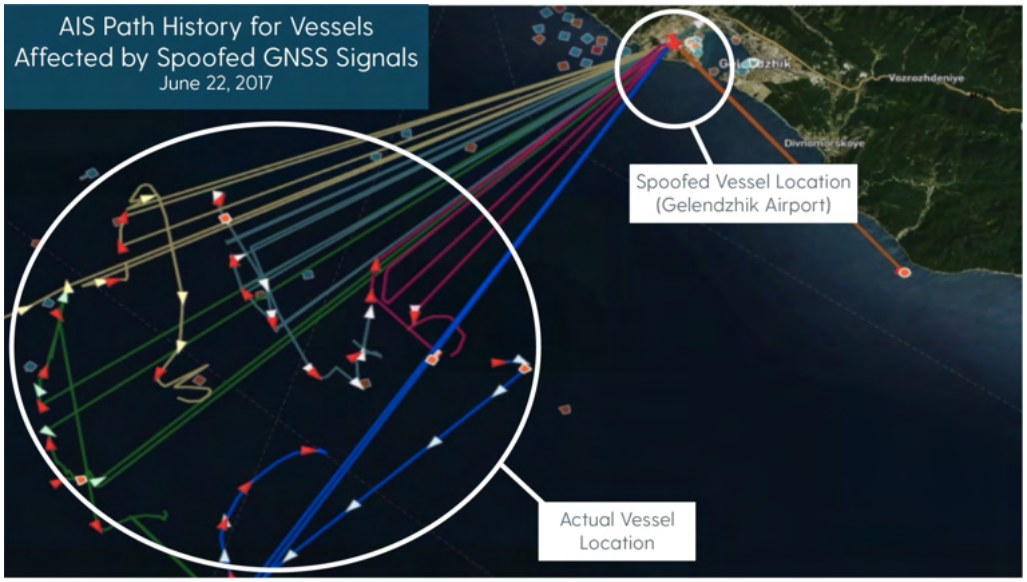


図 4.4: GPS スプーフィングの状況 [4]

4.1.3 GPS ミーコニング

GPS ミーコニング（ GPS Meaconing ）は，正規の GPS 信号を記録し，一定時間遅延させた後に標的の受信機に送信することにより，混乱させる攻撃である．所謂，中間者攻撃のようにあらゆる無線信号を受信・記録し，再生することが可能である RF レコーダを送信用のアンテナを付けることで一度記録した GPS 信号を再生できれば，容易にミーコニングデバイスと

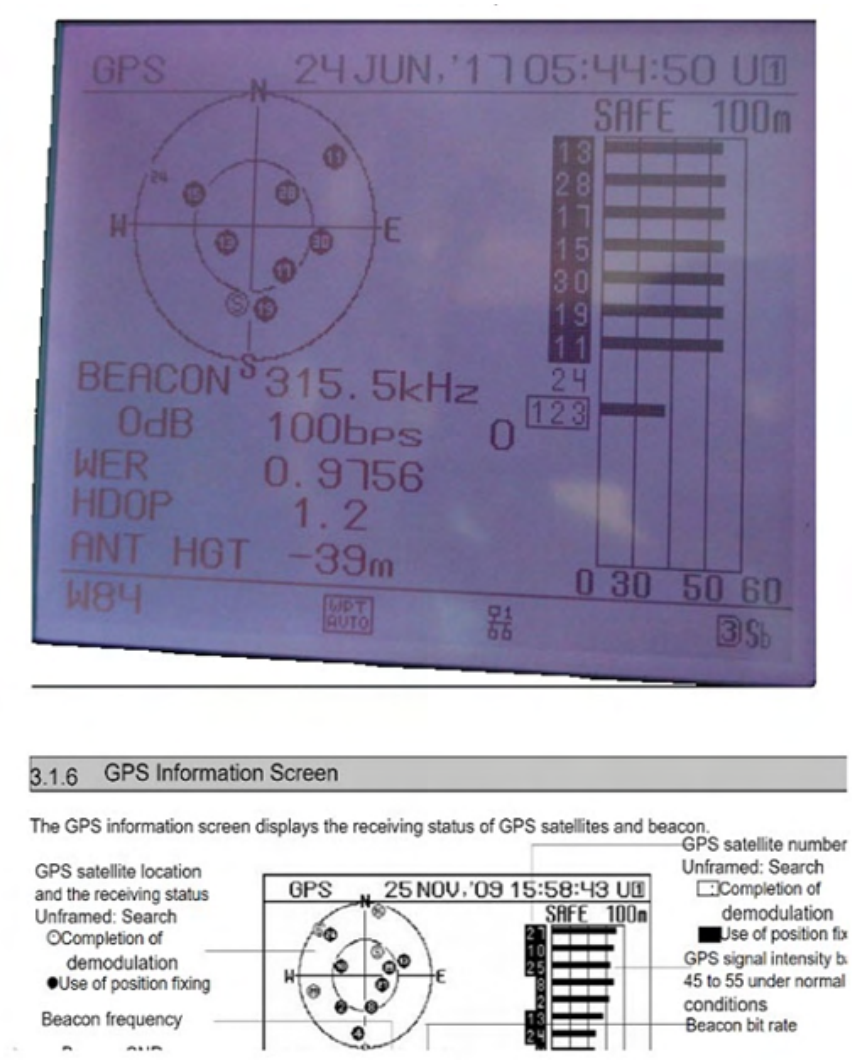


図 4.5: GPS スプーフィングの受けた受信機の状況 [4]

して利用することができる．ミーコニングの対策としては GPS 受信機に内蔵されている時計時刻と GPS 信号を比較・照合することが考慮できるが，GPS 受信機によってその機能が内蔵されているかは異なるため，統一された規格は存在しない．また，再生でもごく短時間の遅延しかないものやリピータによるミーコニングには有効な対策とはならないとされる [51].

4.2　GPS のセキュリティ対策

GPS への攻撃に関するセキュリティ対策として，スプーフィング攻撃に対する民間 GPS 信号の脆弱性について議論されている [47]．また，GPS がどのように動作するかを解説し，GPS 信号の構造について詳しく説明している．Warner[47] らは，スプーフィング攻撃の対策として欺瞞信号を検出するため，GPS 信号強度の監視，衛星識別コードの監視，時間間隔の

確認，時刻のタイミング比較や加速度計を使用してのカウンタチェック等の提案について述べている．しかし，GPS スプーフィング対策の GPS の動作や GPS 信号の構造に即した対策ではあるが，一般的な議論に留まっており，具体性に欠けるものだった．Warner ら [47] の提案は各手法の性能を評価するためのテストが実施されていないため，実証することができていない．また，提案された手法の大部分は，信号特性の監視のみである．

上記以外に以下の対策が提案されている．

1. 信号処理による防御
2. 認証による防御
3. センサヒュージョンによる防御
4. アンテナによる防御

4.2.1 信号処理による防御

標準的な GPS/GNSS 受信機の中に信号処理アルゴリズムとして実装できるスプーフィング検出技術がある．

(1) 信号の歪み検索
(2) 信号の複素相関関数の検索
(3) 総当たり取得検索

(1) の手法は，信号のドラッグオフ中に発生する歪みや混乱を検索するものである．最も単純な技術は，受信のキャリア振幅 A_i，ビートキャリア位相 $\varphi_i\ (t)$ ，またはコード位相 $\tau_i\ (t)$ の不合理な突然のジャンプを検索する方法である．A_i の急激な増加や $\varphi_i\ (t)$，または $\tau_i\ (t)$ の異常な変位は，攻撃の開始時に発生する可能性があるとされる [55]．検索手法としては，RPM (Received Power Monitoring）の受信電力の合計を絶対スケールで監視することである．この手法で必要な事は，すべての受信 A_i 値と受信機 RF フロントエンドの自動利得制御 (AGC：Automatic Gain Control) 設定を見ることである [56]．そして，スプーファーが大幅な電力優位，$A_si \gg A_i$ (すべての $i = 1, \ldots, N$）を必要とした場合，攻撃開始時に総電力が突然増加する可能性がある．特に 1 〜 2 dB 以上増加した場合，突然の電力急増は攻撃示唆の可能性がある．但し，ノイズフロア・スプーフィング (Noise Floor Spoofing) を含むオーバーパワー攻撃に対して脆弱である [57]．

(2) の手法は，受信機がトラッキングループ識別器を合成する時の複素相関関数を詳細に調べる方法である．スプーフィング攻撃の最初のドラッグオフの間，真のコード信号とスプーフィングによる偽のコード信号とキャリア位相の間の不整合により，自己相関関数が歪む．相関関数の歪みを検索するために，典型的な GPS/GNSS 受信機であっても修正することが可能とされる [58]．主な要件は，受信機の信号レプリカと受信信号の間の追加の複素ベースバンド相関を計算することで，これらの相関が，コードオフセット軸に沿った遅延の拡張をセットで計算される．

しかし，複素相関関数の検索には，2 つの欠点がある [55]．1 点目は，自然のマルチパス信号が同様の結果をもたらすことである．そのため，スプーフィング検出器はアラームを発する前に，観測された歪みが単なるマルチパスとして証明できないことを確認する必要がある．2 点目は，スプーファー機器が真の信号を大幅にオーバーパワーした場合，検出性能が低いことである．歪みを回避するために必要なスプーファー機器の出力は，RPM の検出方式で可能である．また，その他の課題として，検出時に過渡的な性質があることである [55] が，ドラッグオフ時に攻撃を検知できなかった場合，(1)，(2) 手法はいずれも攻撃の検知機会を逸してしまう可能性がある．

(3) の手法は，追跡したすべての信号の再取得を常に試みることである．各信号に対して，コード位相と搬送波ドップラーシフトの全範囲を総当り的に取得探索 (ブルートフォースアクイジションサーチ) する．しかし，ブルートフォースアクイジションサーチは，受信機に大きな信号処理負荷をかける．そのため，1 つの合理的な方法は，追跡された信号の追加インスタンスを，一度に 1 つの信号について，順次検索することである．受信した信号の第二版が検出された場合，受信機を初期取得モードに戻し，再びブルートフォースサーチにより全信号の全インスタンスを検索する．その後，受信機は偽装された信号から真の信号を選別し，ナビゲーション機能を回復させることを試みる．しかし，この手法は，過度に強力なスプーファー機器によって，真の信号を妨害し，再検索中に検出できなくされ，手法が破られる可能性がある．強力なスプーファー機器に対しては，RPM の方式が検出に有効であると考えられている [55]．

4.2.2　認証による防御

スプーフィング対策の一つとして，GPS 衛星が送信する測位信号の認証化が考えられている．これは暗号化と復号に非対称の鍵ペアを用いる公開鍵暗号方式により，欺瞞信号の判別をするものである．すでに仕様が公開されている GPS 信号に対して採用することはできないが，他の衛星航法システムでは採用されつつある [43]．具体的には，復号に用いる公開鍵についてはあらかじめ利用者に周知 (受信機に搭載) され，この公開鍵で正しく復号できる信号であれば，公開鍵に対応した秘密鍵を保有している運用者により生成されていることが保証される．但し，復号した結果として得られる情報の形式が既知であり，情報量が多くないこと，一方向通信なので鍵ペアを任意には変更できないことなどから，認証としての強度を保つことは難しい．一方で，GPS 衛星が送信する測位信号の暗号化 [51] も考えられているが，機密性な情報は信号に含まれていないことが必要性がないと考えられる

4.2.3　センサヒュージョンによる防御

GPS 受信機 (アンテナ) の物理的な移動状況がわかれば，欺瞞の有無を知ることができる．このためには，GPS 以外の位置センサと比較することが有効である [51]．さまざまなセンサが考えられるが，船舶には，前述したとおり，IMU (ジャイロコンパス) を筆頭に多くのセンサを搭載しているため，他の乗物に比べて信号の比較は容易と考えられる．

4.2.4　アンテナによる防御

過去の事例のスプーフィング及びミーコニングの特徴として，攻撃者は地上付近から送信してくることが予想される．そのため，本来 GPS の受信アンテナは無指向性であるが，指向性をもたせることで，GPS 衛星が実際に存在する方向から到来する電波だけを受信するようにすることが対策となる (**図 4.6**)．しかし，一般的な指向性アンテナはパラボラアンテナであるが大型となるため，複数のアンテナを用いてアレイアンテナによる受信方式が主に検討されている [51][59]．3 次元の指向性を実現するためには最低でも 3 式のアンテナを配置する必要があるため，携帯機器での採用は難しいものと思われる．

また，攻撃者が GPS 衛星と同じ位置にアンテナを設置することは不可能である．したがって，特定の地点の GPS 受信機に対してスプーフィングやミーコニングを実行したとしても，離れた地点の GPS 受信機に対しては同様の効果は得られない．すなわち，広い地理的範囲の GPS 受信機に対して矛盾のない欺瞞信号を作り出すことは原理的にできないため．多数の GPS 受信機によるネットワークを用いることが提案されている [51]．ネットワークに参加している GPS 受信機が得た測定値を比較し，矛盾を検出するのである．さらに，GPS 受信機同士が測定値を交換して互いに比較を行うことも考えられており，自律的な欺瞞検出方式として機能するものと思われる．但し，比較するための受信機の設置場所は，別途送受信する必要があるため，厳しい場合がある．

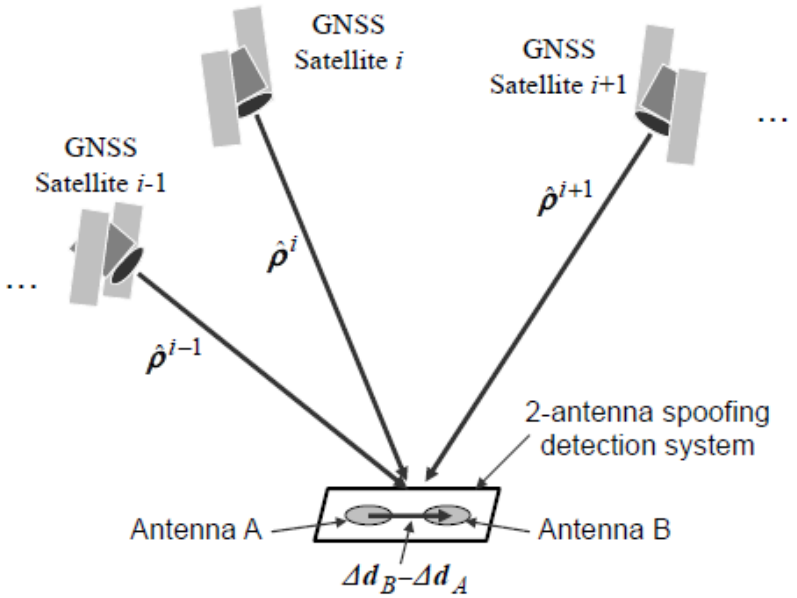


図 4.6: 2 アンテナベースによる典型的な信号到着形状のスプーフィング検出 [55]

4.3　既存のセキュリティ対策の課題

4.2 節で述べたように，GPS への攻撃の対策は，主に検知等の多岐にわたって研究されていたが，既存の航海システムへの適用は進んでいない．GPS に依存する航海システムへのサイバー攻撃に対するインシデントレスポンスについては，航海士の訓練の試行として実際の船舶を使用したインシデントレスポンスの実験が行われている [60]．

船舶の運航は，海洋における外的な環境影響 (例えば，風波浪や船舶交通など) が大きいため，その運航の可用性，並びに継続性が非常に重要であり，対応できなければ安全な運航を継続できない．そのため，OT 機器系のサイバーセキュリティ対策の必要性が高いが，その適用は余り進んでいない．したがって，運航者 (航海士) のサイバー攻撃に対するインシデントレスポンスに関する検討が必要であり，それらの検討を基にした情報セキュリティインシデントに対する関係者との共通理解を促し，対応できなければ，可用性や継続性を失いかねない．また，**1.1 節**で述べたとおり，自動化や自律化が進んでいる中において，この知見に関する検討は重要だと考えられる．

第 5 章

提案手法

船舶の GPS に対する電波攻撃はが行われた場合，攻撃の有無を検知することは既存の航海システムでは非常に難しい．本章では，電波による船舶への GPS 攻撃に対する検知及び対処方法を検討するために，操船術，航海術並びにそれらに係る航海システムの整理を行う．

整理結果からとるべき対処フローを導き出し，乗組員 (航海士，または通信士) が攻撃を受けた場合の適切な対処の流れを提案する．

5.1　航海システム・操船術・航海術の整理

航海術のなる航法の測位性能を比較し，それらの運航者 (航海士) のツールとなる航海システムの整理を行い，その適用について検討する．なお，GPS を含む GNSS は，本来であれば電波航法のひとつであるが，選択する手法を分けるために，電波航法と別手法として取り扱うこととする．

5.1.1　航法別における測位性能の比較

2.2 節で述べた航海術において，各航法により絶対位置として位置情報を取得できる手法が**表 5.1** となる．なお，ロランシステム等の電波航法は，上空からデータを交信できる GPS を含む GNSS 衛星に比べて，システムの更新は行われていないため，測位性能は GPS 等に劣る．また，位置取得をカバーできるエリアがサービスを提供している国に依存しているため，適用範囲においても劣る上に，**2.2.4 節**で述べたとおり，多くの国がサービス提供を廃止している．

また，**2.2 節**で述べた航海術において，各航法により相対位置として位置情報を取得できる手法が**表 5.2** となる．目視は，船舶の乗組員である航海士による目測であり，実際の海域の状況や各システムと航法を選択・比較することで，操船の判断を行うこととなる．

表 5.1: 航法別における測位性能の比較 (絶対位置)

手法	精度	適用範囲	備考
GNSS	1 m	遮蔽物がない場合	-
電波航法	100 m 程度	約 1,000 km	多くが廃止
地文航法	185 m 程度	約 約 60 km (場所に依存)	海図が必須
天文航法	185 m 程度	目視範囲	天候に影響

表 5.2: 航法別における測位性能の比較 (相対位置)

手法	精度	適用範囲	備考
慣性航法	300 m 程度	制限なし	状況に依存
目視	100 m 程度	視界良好時に限る	-

5.1.2　カテゴリの整理

各システムと操船術及び航海術を図 **5.1** のとおり，4 つのレイヤーに分けた．「レイヤー 4」が，船舶の位置取得における各システムと操船術及び航海術のフルスペックとなり，「レイヤー 4」→「レイヤー 3」→「レイヤー 2」→「レイヤー 1」に移行するごとに取り得るシステムと航法の選択肢が減っていくこととなる．

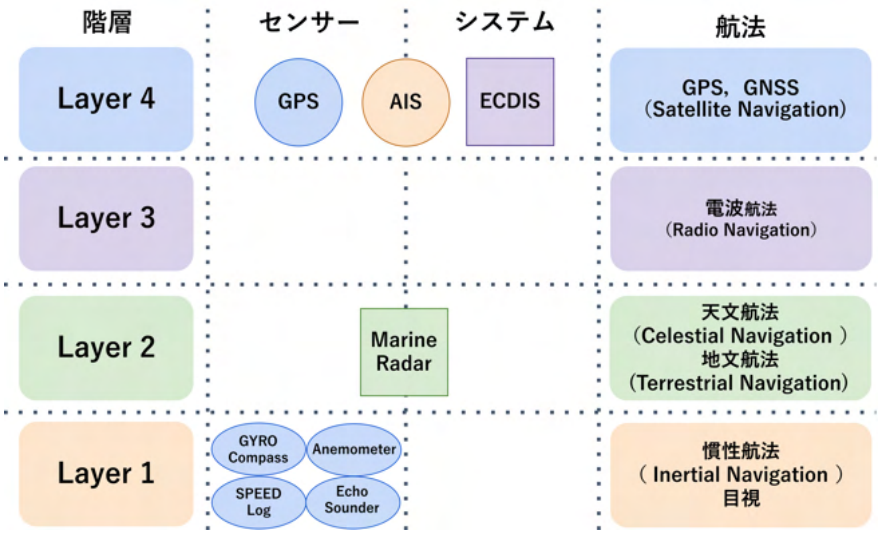


図 5.1: 航海システム，操船 (航海術) におけるカテゴリ (レイヤー分け)

5.2　GPS 攻撃に対するレスポンスチャート (提案フロー)

船舶を運航する航海士は，航行している海域や状況に応じて**第 2 章**で述べた操船術・航海術を適切に選択することで船舶を安全な位置に航行する必要がある．航海士は，現在の船舶の状態から，どの操船術・航海術を適用するか選択しなければならない．しかし，現状，GPS への攻撃された場合，どの航法を適用し，どのツールを使用するかは，各々の航海士の経験則に依然しており，未だ議論されていない．そこで，本研究は GPS ジャミング・スプーフィングによる攻撃を受けた場合の対処フローを提案する．

船舶の状況を **(A)** 〜 **(D)** の 4 つの状況を想定し，**図 5.2**〜**図 5.5** に示すフローの適用を提案する．そして，すべての対処フローを総合して，**図 5.6** の適用を提案する．

(A)　**GPS 使用不可**

まさに，GPS への攻撃が行われ，GPS からの位置情報が取得できない，または位置情報が改竄され正しい位置を示していない状態である．

(B)　航行している海域 (外洋 **or** 近海)

(1)　外洋で **GPS** 攻撃を受けた場合 (陸地を視認することができない広々とした海域)

想定される攻撃について，陸上からの攻撃については出力が大きい電波によるもの．海上からの攻撃は近くを航行する船舶・航空機等による可能性が高い．攻撃を受けた船舶は位置を見失い，方角しかわからない状態となる．

(2)　近海で **GPS** 攻撃を受けた場合 (陸地に近い海域，地物 (灯台等) が視認可能)

海上または陸地に関わらず，容易に攻撃を実行しやすい (低出力で良い)．東京湾等の船舶が輻湊する海域．攻撃が成功すると船橋内は混乱し，判断の遅れが命取りとなる．

(C)　天候

天文航法を適用している船舶は，航行している海域の天候が「晴れ」以外だった場合，太陽，惑星を視認することが不可能である．

(D)　視界の状況

濃霧，豪雨等により船舶の船橋から海上の状況を視認できない．視界不良のため，船舶の位置情報を取得するには，慣性航法を適用することで，船舶の進行している方位から計算・推測する．

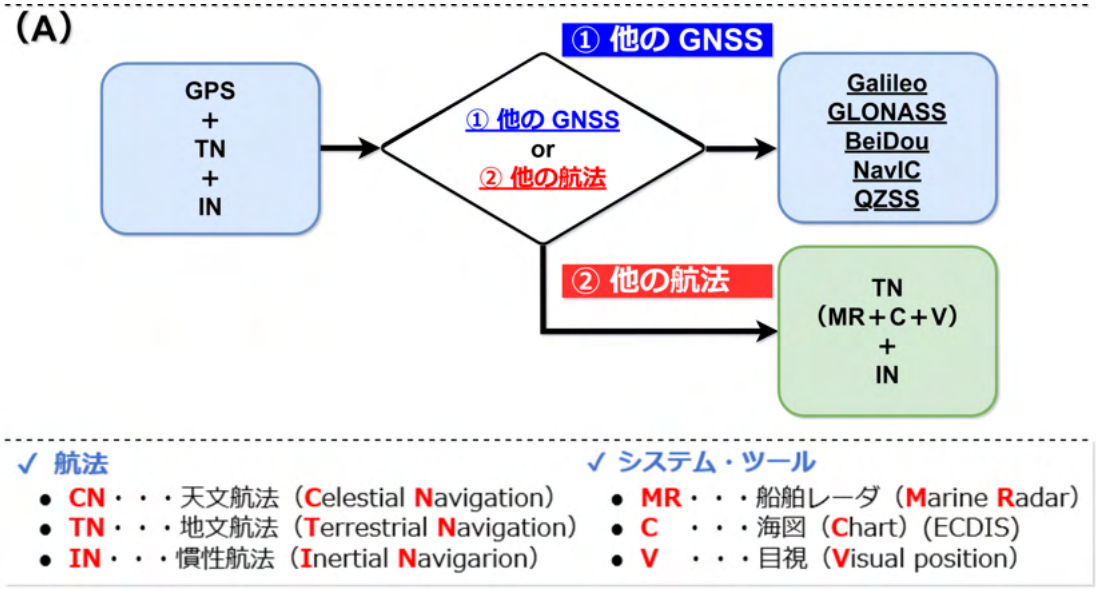


図 5.2: (A)GPS ジャミング・スプーフィングに対する対処フロー (GPS の使用不可)

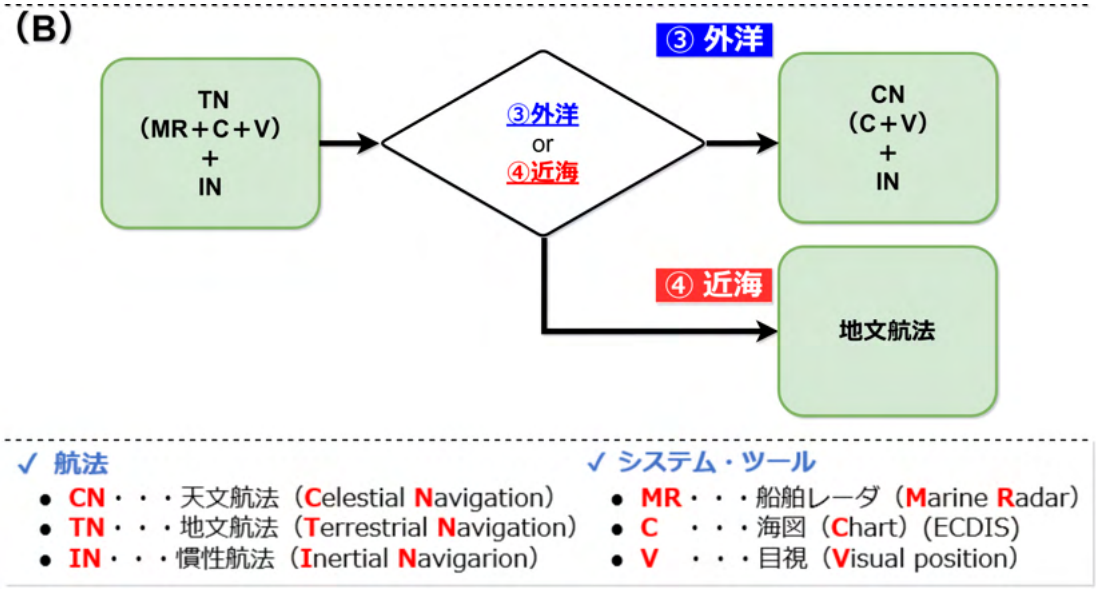


図 5.3: (B)GPS ジャミング・スプーフィングに対する対処フロー (航行している海域)

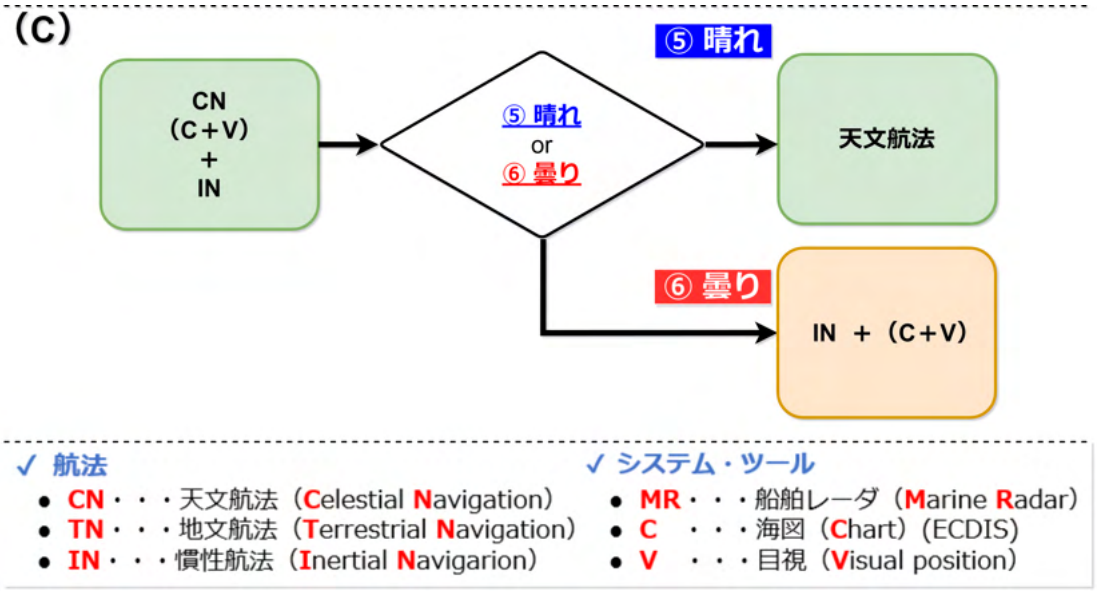


図 5.4: (C)GPS ジャミング・スプーフィングに対する対処フロー (天候)

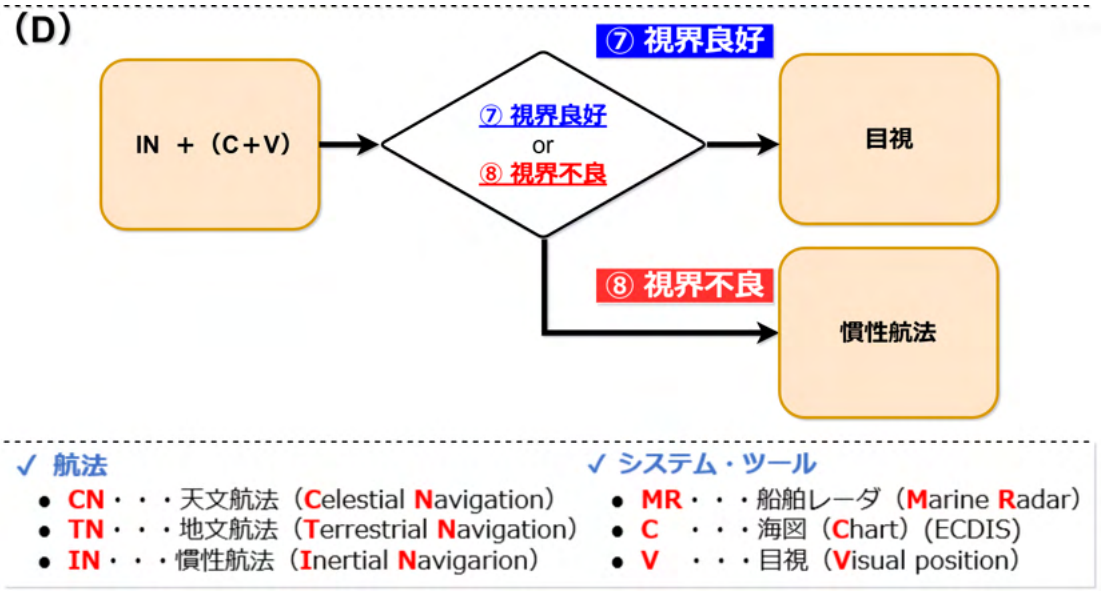


図 5.5: (D)GPS ジャミング・スプーフィングに対する対処フロー (視界の状況)

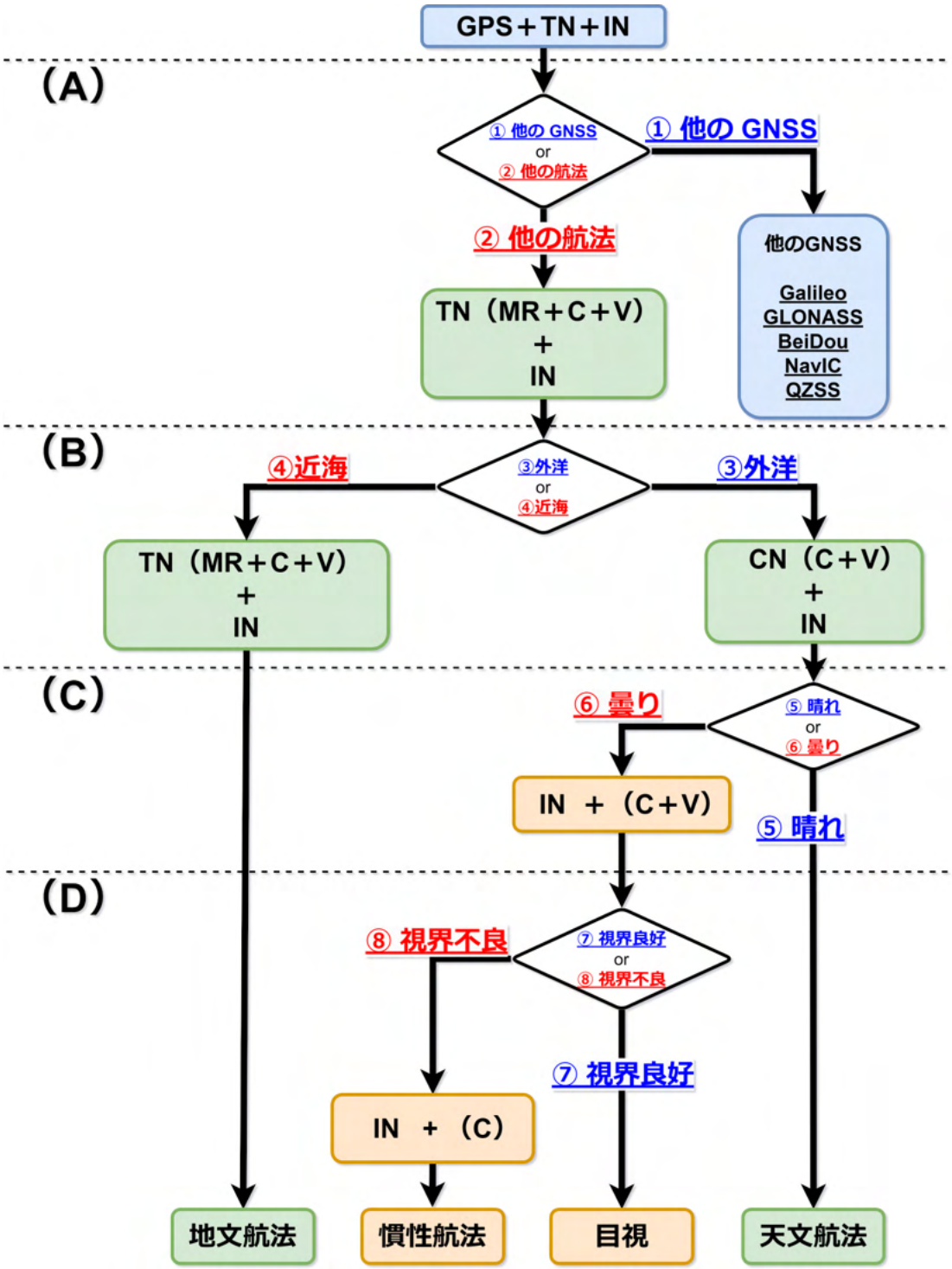


図 5.6: GPS ジャミング・スプーフィングに対する航海士がとるべき対処フロー

第 6 章

評価

GPS の電波を利用し，最も船舶への影響が多く出ると考えられるスプーフィング攻撃が航海中に発生すると想定とした場合の船舶の運航への影響性や不安全な事項の確認，また図 **5.6** に示すフローチャートの類似性について，実験を行い評価する．

6.1　攻撃実現性

現場でジャミング，スプーフィング，ミーコニングの攻撃の実現に関する可能性について，まだその評価は多くない．携帯電話や自動車のような最も一般的なタイプの受信機に対する攻撃は，攻撃者にもたらされる利益のリターンに対して難易度が高いため，現実的ではない．

一方で，船舶，飛行機，発電所等の攻撃対象は，依然としてより高い価値がある．

6.1.1　実行コストと労力

コストは，構築される攻撃ツールとなる GPS ジャマー機器，・スプーファー機器の仕様と攻撃対象のタイプに依存する.**4.1** 節で説明した GPS ジャマー・スプーファー機器の仕様に従って，シミュレーション及びデバイスに関連する実用的なコストで評価する必要がある．その多くは，今のところ理論的なものに過ぎない．但し，簡素な GPS ジャマー機器については，数万円程度の安価で入手が可能である [51].

6.1.2　シミュレータの必要コスト

正規の信号と同期させることなく，少なくとも 1 つの GPS 衛星を送信 (ブロードキャスト) することは，労力の点で最も安価な方法である．1 機，または複数の GPS 衛星を生成するソフトウェアは，シミュレータ・メーカーが提供する．アナログとデジタルの 2 種類がある [61]. アナログのものは，各衛星を表現するために個別の送信機が必要であるため，非常に高価になりがちで，最高で 50 万ドルにもなるとされる [61].

6.1.3　ミーコニングの必要コスト

ミーコニングを実現するための機器ミーコナーを作ることについては言及されているものは余り多くない．しかし，2,300 ドルで販売されているソフトウエア無線機 (SDR:Software Defined Radio) と，700 ドルの追加費用による広帯域トランシーバーをベースにしたミーコナーを作ることは比較的簡単だと予想される．これを GPS アンテナから捕捉した信号と組み合わせ，遅延後に再生することもできる [55]．しかし，SCER (Security Code Estimation and Replay) のために可変遅延を導入したり，様々な衛星信号の分離には，ソフトウェアの開発が必要となり，最終的なコストは，おそらく安価なフル・シミュレータに近づくと想定される．

6.2　実験

6.2.1　実験環境

GPS スプーフィングによる運航への影響性や不安全な事項の確認，**図 5.6** に示したフローチャートの類似性について明らかにするための実験を実施した．本研究では，広島商船高等専門学校[*1]の協力により操船シミュレータ装置を利用し，GPS スプーフィングに関するシミュレーションを実施，その際に運航の経験のある航海士にシミュレーションを依頼し，検討することとした．シミュレーションは，**図 6.1** に示すように，航海当直を行う航海士役及び，操舵システムを動かす操舵役の 2 名で当直を行う体制で実施することとした．この状況は一般的な海域における一般的な交通状況での当直体制である．

今回，GPS スプーフィングされたシナリオを構築し，その際の，航海士の行動と航海の軌跡，並びにアンケート調査を通じて，航海システムへの影響を図るものである．実施にあたって，公益社団法人日本心理学会倫理規程を踏まえた上で，被験，並びにアンケート調査を行った．

なお，実験環境の構成については**表 6.1** に，アンケートの項目は**表 6.2** に示す．

[*1] 広島県豊田郡大崎上島町にある日本の国立高等専門学校．商船学科，電子制御工学科，流通情報工学科，専攻科：https://www.hiroshima-cmt.ac.jp/

図 6.1: 操船シミュレータでの実験 (被験) の様子（被実験者 (前) と操舵者 (後))

表 6.1: 実験シミュレータの構成

No.	システム	図
1	船舶レーダー	**図 6.2**
2	ECDIS	**図 6.2**
3	操舵システム	**図 6.3**
4	国際 VHF システム	**図 6.4**

表 6.2: 被験者へのアンケート項目

No.	質問事項
Q1	GPS スプーフィング攻撃に対して反応または把握できたか
Q2	GPS スプーフィング攻撃をどのタイミングで反応または把握することができたか
Q3	GPS スプーフィング攻撃に対して反応または把握できたときの心境
Q4	GPS に依存しない運航にためらいなく移行することができたか
Q5	GPS 使用不可以降の航海システムの移行先は何か
Q6	GPS 使用不可以降の航海システムの移行先は何か (問 5 での回答以外に使用したものがあれば回答する)
Q7	その他特記すべき事項 (自由記述)

図 6.2: 操船シミュレータの構成【船舶レーダー (左)，ECDIS (右) 】

図 6.3: 操船シミュレータの構成【操舵システム】

図 6.4: 操船シミュレータの構成【国際 VHF システム】

6.2.2　実験シナリオ

シナリオは，過去の船に対するインシデント事例 [2]，攻撃にかかる実行コスト，労力，利益，並びに影響度を総合的に検討した結果，船舶へ直接的な攻撃される可能性は非常に低い．そこで，本実験は，甚大な被害になると思われる国民の生命及び財産を守るために存在する「軍事基地」，または生命及び経済に多大な被害を受ける「空港」等に対する攻撃となるテロ攻撃を想定した．従って，過去の船舶に対するインシデント事例に非常に環境が似ている「神戸港ポートアイランド」及び「神戸空港」周辺とした．神戸港を実験海域とした．

- 軍事施設等の物理セキュリティや**テロ攻撃** (過去事例の傾向)
- 航空機やドローン等への攻撃 (**影響度が高い**)
- **船舶への直接攻撃は低いが，副次的 (二次被害) 被害**の可能性

時間は 12:00 スタート (昼間) とした．対象となる船舶は 1000 GT 級の一般貨物船とした．対象の実験海域を**図 6.6** に示す．GPS のスプーフィングの原因となるアンテナ位置を，ポートアイランドの堤防上に設置した想定とし，スプーフィングの範囲は，黄色帯とする．

対象とする船舶は，開始点から 220 度方向に運航した後，265 度方向に変針し，しばらく直進して終了するものとした (**図 6.6**)．この間に，横切り船，速度の遅い同航船，反航船，漁船など 8 隻の他船が同時に運航している交通環境とした．その様子を**図 6.7** に示す．国際 VHF 電話システムにて，他船，並びに海上交通センター (Vessel Traffic Advisory Service Center) [*2]に連絡できるように想定した．VHF の連絡相手 及び 交通の見合い関係整理は，シミュレータのオペレーターが行うものとした．航行は，各種法規に従うものとして，従えない場合はシナリオを中断した．

GPS スプーフィングの内容は，スプーフィング範囲内に船舶が入った際，0 度方向 (北方向) に 300 m 程度に GPS の位置をずらし，範囲を外れると元に戻すものとした (1 度目のスプーフィング)．さらに，終了点付近で 45 度方向 (東方向) に 30,000 m 程度の大幅に船舶の位置をずらすものとした (2 度目のスプーフィング)． 航行は，10.5 kts で航行し，このシナリオでは，増速，並びに減速は，非常時以外は行わないものとした．GPS スプーフィングによって，船舶レーダーで重畳している AIS データにも影響が出る設定としている．

本シナリオについて，神戸沖第一号灯浮標と神戸沖第二号灯浮標の間を線より上を航行することを推奨されており (本灯浮標は船舶の交通流の整流性を持たせている)，北に 300 m のずれは，これを見ながら航行した場合，想定よりも船は南側を航行してしまうため，安全ではない位置を航行することとなり，正面衝突の事故を引き起こしやすくなる．そのため，このシミュレーションによる評価の基準として，航走している軌跡が神戸沖第一号灯浮標と神戸沖第二号灯浮標の間を線より上を航行しているかどうかで判断をする．

[*2] 海上保安庁により日本の 7 箇所に設置．海上交通安全法，港則法で定められた船舶が通行する航路・輻湊海域において，船舶の安全運行に必要な情報の提供と航行管制を一元的に行う．https://www.kaiho.mlit.go.jp/soshiki/koutsuu/toudai/center.html

実験の被験者について，1000 GT 級の船の船長を務めることができる 3 級海技士 (航海) 以上の海技免状を所持し，乗船経験が 1 年以上の航海士とした．また，「実験海域への航海経験がある」，または，「運航船での実務経験がある」かにおいて分類をし，**表 6.3** に示す．また，すべての操船者は，日本で教育を受けた，日本人海技者である．

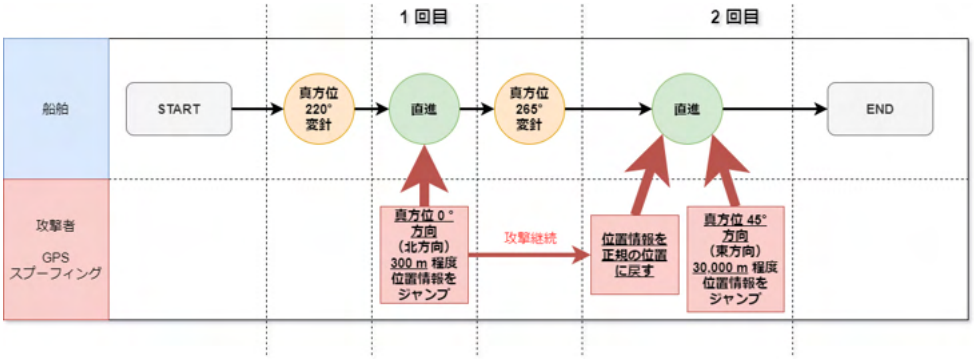


図 6.5: 実験の流れ

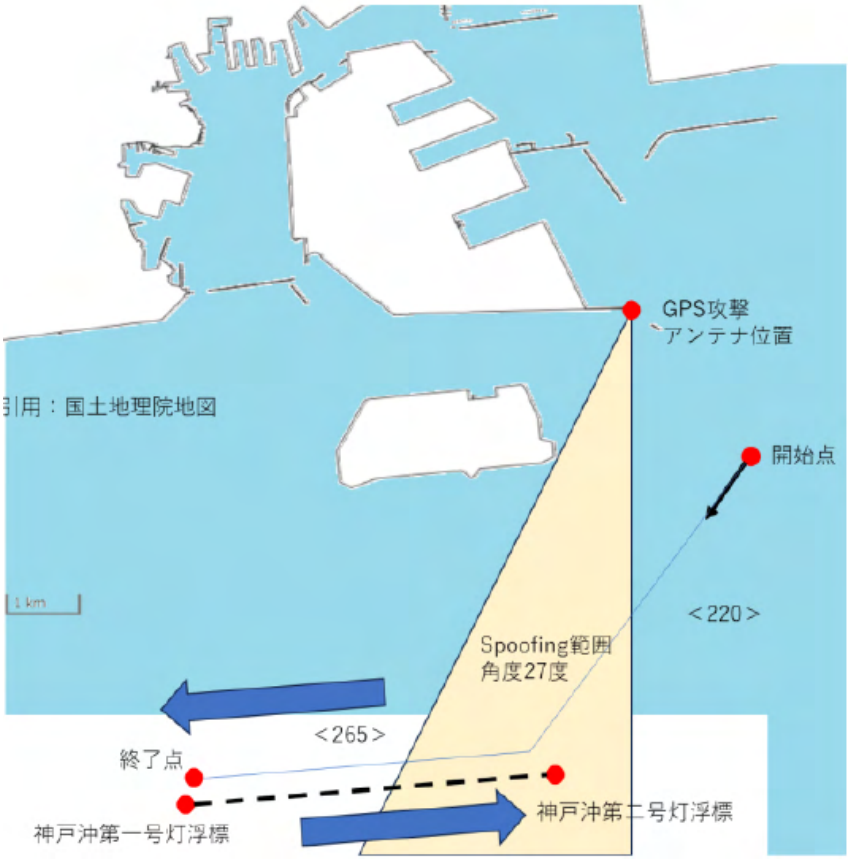


図 6.6: 実験の海域

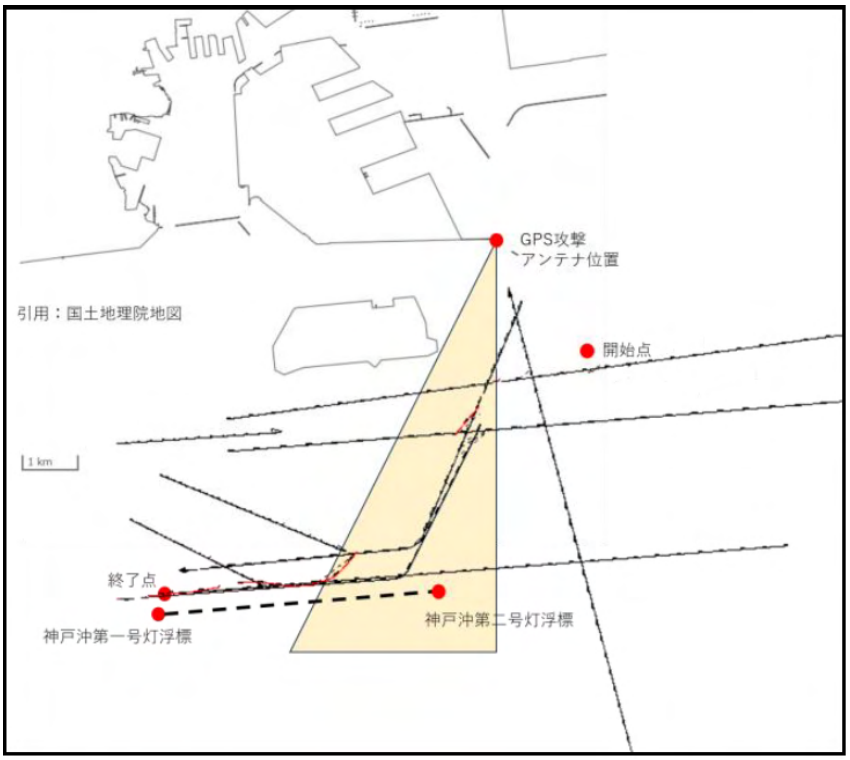


図 6.7: 他船の航行状況

表 6.3: 被験者の経歴等について

被験者	実験海域での航海経験	運行船の実務経験
A	有り	5 年以上
B	有り	5 年以上
C	無し	5 年以上
D	有り	1 年以上 5 年未満
E	無し	1 年以上 5 年未満
F	無し	1 年未満
G	無し	1 年未満

ところで，航海システムに入る GPS データフォーマットに異常が生じた場合，正常な GPS データがシステムに入力されないため，AIS，船舶レーダー，ECDIS 等のシステム自身からは，GPS データ異常を示すエラー警報が出力される．もし，ひとつのシステムのみの警報ならば，警報が出力された対象システムのみの障害が予想される．つまり，GPS ジャミング攻撃を受けた場合は，正常な GPS データを受信できないため，すべてのシステムから同時にエラー警報が出力されることとなる．

一方で，GPS スプーフィング攻撃を受けた場合は，位置情報の改竄であることから，GPS データフォーマットに異常がある訳ではないため，入力される航海システムからはエラー警報が出力されない．したがって，GPS スプーフィングによる攻撃は，**図 6.8** に示すとおり，エラー警報を出力されることなく，ECDIS に表示される自船及びレーダー画像と電子海図 (ENC) との間にずれを生じさせる．よって，これが船舶を運航する航海士が GPS スプーフィング攻撃を受けている可能性に気づく端緒となる．

図 6.8: GPS spoofing の様子

6.3　実験結果・考察

6.3.1　船舶の航跡結果

操船シミュレータで船舶を運行した航跡結果を**図 6.9** に示す．**図 6.9** の航跡結果から，被験者 7 名全員が神戸沖第一号灯浮標と神戸沖第二号灯浮標間の線より上を航行することができていたこと．したがって，安全に航行をしていることが明らかであることから，提案したレスポンスチャートが類似していると推定される．しかし，2 例ほど，終了点前で状況の大きな変化がなく終了したため，北へ流れた形の航跡となった．

6.3.2　アンケート調査結果

次いで，被験者 7 名に対して被験後に**表 6.2** のアンケートを実施した．アンケートの結果を**表 6.4** に示す．**表 6.4** によると，GPS スプーフィング攻撃に対して，反応・把握できたと回答した被験者は 6 名，気づかなかったと回答した被験者は 1 名であった．しかし，この結果は，GPS スプーフィングの北方向に 300 m のずらす 1 度目の攻撃によって，スプーフィングを受けたことに気づいた被験者はおらず，2 度目の攻撃で漸く気づくことができたものである．また，気づい要因は変針後の ECDIS の確認や船舶レーダーの挙動で把握できたものである

船舶の航跡結果とアンケート結果から以下の 2 点が推測される．

1. 内航経験者への細やかな位置変化を与える GPS スプーフィング攻撃は，影響が少ない．
2. ECDIS を優先的に確認する傾向のある航海士は，GPS スプーフィング攻撃の影響を受けやすい．

1 点目は，GPS スプーフィングを 300 m 程度の僅かな位置変化による攻撃は，影響性が少ない可能性が推測される．これは，内航経験が主な航海士において，地文航法 (海図のクロスベアリングを活用した航法）及びレーダー航法 (船舶レーダーを活用した航法）を主に行っており，ECDIS (電子海図) の GPS の位置を留意せず，航海をしていることが考えられる．したがって，こうした影響性が少ないと考えられる．しかし，逆の見方によっては，既に，提案したレスポンスチャート (**図 5.6**) における，**「Layer1」**及び**「Layer2」**に移行している可能性が高く，通常の国内を航海する，特に沿岸航行を行っている航海士の行動として，提案したレスポンスチャートは違和感なく実施できるものであると推測される．また，交通流が多い海域においては，船舶の見合い関係を目視で把握する必要があり，その際に周りの風景や海図を用いたクロスベアリングをしなければ，安全に航海ができないため，目視を重視する傾向が見られたのだと考えられる．

一方で，2 点目は ECDIS を注視して航行していた被験者が GPS スプーフィング中に自己位置の認識を誤り，航行予定航路から大きく外れ，後の対応が慌てるケースが 1 例確認された． これは，船舶を運航する上で，前述の目視を重視する傾向が見られる内航経験が主な航海士と異なり，多くの情報を把握することができる ECDI に信頼を置き，優先的に確認する

傾向にあったために生じたのだと推測される．

また，その他に留意すべき項目として，GPS に大きな変位を伴う東方向へ 30,000 m 位置をずらす 2 回目の GPS スプーフィング攻撃においては，異常に気付き，取り扱い説明書等を確認しながら対応する例が見られた．，さらに，海上交通安全法適用海域，すなわち，適切な航海システムを使用しなければならない海域へ入る前における航海士の行動として，海上交通センターに「航海システムの異常」を，国際 VHF 電話システムを使用して，通報する例が見られた．この行動は，過去の関連研究等にも前例があり [4][52]，慣習的に実施される可能性があることが推測される．海上交通センター以外にも他船との確認の手段として，国際 VHF 電話システムが使用される可能性があり，このような事実確認や通報するのための通信は，多くの船舶が航行する海域で，より通信が増加する可能性が推測される．その結果，遭難通信や緊急通信の無線周波数を塞ぐこととなり，船舶間同士，船陸間同士で一時的に通信不能に陥る可能性が想定される．こうした二次的な被害を生じる可能性があるため，海上交通センターは留意する必要があると推測される．

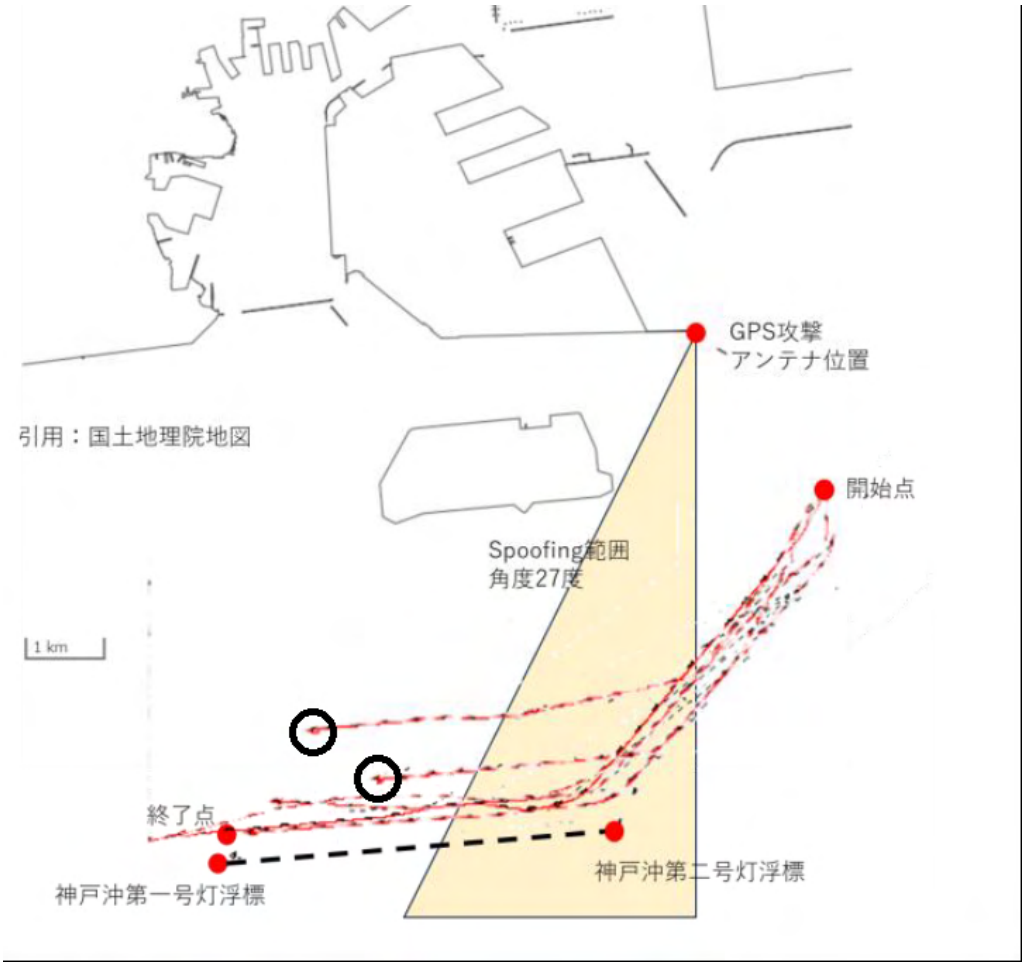


図 6.9: 船舶の航跡 (航海の軌跡：赤い点線)

表 6.4: 実験後の被験者へのアンケート結果 (1/2)

No.	質問事項	概要	結果
Q1.	スプーフィング攻撃に対して反応または把握できたか	反応または把握できた.	6
		反応または把握できなかった.	1
Q2.	スプーフィング攻撃をどのタイミングで反応または把握することができたか	大きく飛ばされたとき (2 回目のスプーフィング) はわかったが，絶妙なスプーフィグ (1 回目のスプーフィング) は全然分からなかった. 自船が消えたことは把握したが，攻撃とは思わなかった. 船舶レーダーの挙動がおかしいと感じた. 船舶レーダーも ECDIS も特段見ていなかった. 変針後，自船の位置を把握するために ECDIS 画面を確認したときに把握できた.	
Q3.	GPS スプーフィング攻撃に対して反応または把握できたときの心境	恐怖を感じた	0
		焦りを感じた	3
		何も感じなかった	2
		その他	2
Q4.	GPS に依存しない運航にためらいなく移行することができたか	移行できた	5
		移行できなかった	2
Q5.	GPS 使用不可以降の航海システムの移行先は何か	その他の GNSS	0
		地文航法	2
		電波航法	0
		天文航法	0
		慣性航法	0
		目視	4
		その他	1
Q6.	GPS 使用不可以降の航海システムの移行先は何か (Q5 での回答以外に使用したものがあれば回答する)	他の GNSS	0
		地文航法	1
		電波航法	1
		天文航法	0
		慣性航法	0
		目視	0
		その他	3
		回答なし	2

表 6.4: 実験後の被験者へのアンケート結果 (2/2)

No.	質問事項	概要	結果
Q7.	その他特記すべき事項	ECDIS や船舶レーダーに不具合が起きたことに気付いたが，神戸が走り慣れた場所だったこともあり，特に対処しようとは思わなかった． 明石海峡航路は難所であるから，船を安全に航海することを第一に考えた．人手があったら，ECDIS に起きた不具合を解決したと思う．普段は，自分の目で見たものと方位を海図に照らし合わせて航海している． 明石海峡航路に入る手前で ECDIS や船舶レーダーに不具合が起きたため，このまま航海してよいかわからず，確認のために VHF で大阪湾海上交通センターに連絡をした． 船舶レーダーと ECDIS を再起動した． エラーの原因を探るため，船橋内に船舶レーダーと ECDIS の取扱説明書がないか探した．取扱説明書を読み，エラーが解決しなかった場合，メーカーに電話して解決しただろ． コースラインを意識するより，周囲の船舶の動向でコース設定を頻繁に変えるので，あまり危機感を感じなかった． 今回は実験前に水深や険悪物がなかったことを海図で確認していたため，船位についてはあまり重視しなかったが，事前に確認ができないあるいはそのような海域であれば，違った結果になったかもしれない．	

第 7 章

まとめと今後の課題

本研究は，電子海図表示システム (ECDIS・ECS）を活用した運航において，最も脅威となる GPS 電波のスプーフィングによる自船位置の変更が，その取扱う航海システムへの影響と GPS スプーフィング後の対応についてレスポンスチャートを提案し，その類似性を日本で教育を受けた日本人海技者を対象に運航シミュレーション利用した実験を通じて，明らかにすることを目的とした．

本研究の結果から下記の知見を得られた．

- サイバー攻撃の脅威について知識が十分ではない日本人海技者は，GPS スプーフィングに対して，反応できない・把握できないとしながらも，GPS に依存しない運航に躊躇なく移行できたこと，そして安全な運航を継続できることが明らかになった．
- 一方で，レスポンスチャートを把握していない状態で，かつ ECDIS に依存していた日本人海技者は，状況を把握できずに安全でない運航を行った事例等も確認された．
- GPS スプーフィングによる被害がある場合，その被害船は通報等ために，国際 VHF 電話システムを使用した，船舶と海上交通センターの船陸間，並びに船舶間の通信が増加する可能性がある．

これらの結果から，**図 5.6** に示すレスポンスチャートの類似性を確認することができた．今回のレスポンスチャートは，今後自動化の進む船舶の運航について航海士 (運航者) に求められる重要な施策であると考えられる．

一方で，本研究における今後の課題として，主に以下が上げられる．

- 近海での航行経験が少ない運航者の対応
- 航法を移行するタイミングに要する時間
- 他のセンサに異常が生じた場合のインシデントレスポンス
- 他の GNSS のセキュリティ対策

本研究の実験の被験者は，実験海域での航海経験や運行船の実務経験に差はあれど，日本人海技者のため，航路のルールや訓練対象の海域は日本列島の周辺海域が主となる．一方で，日本の近海での航行経験が少ない外国人海技者等が，本実験を被験した場合，ECDIS に依存し

ていた海技者と同様に状況を把握できずに安全でない運航を行った可能性が高くなると考えられる．

本研究の実験は，提案するレスポンスチャートと GPS スプーフィングに対する海技者の行動の類似性を検証したものであるため，厳密な行動の検証を実施していない．よって，航法移行のタイミング (時刻)，要する時間等を検証することで，ジャミングを含む電波妨害を受けた場合の詳細な対策を導くことができるのではないかと考えられる．

被験者が GPS スプーフィングを検知する端緒として，地文航法を適用するためのツールとなる船舶レーダー，慣性航法の適用に必要であるジャイロコンパスが使用できなくなるサイバー攻撃が起こった場合，既存のシステムだけでは安全性を確保できない可能性が高くと考えられるため，GPS 以外のセンサ類に異常が発生した場合のインシデントレスポンスについて想定する必要があると考えられる．

GNSS の今後の進展として，2024 年度から提供予定の QZSS 信号認証サービス [43] により，GNSS 受信機で受信した信号が測位衛星から送信された真の信号であるかを確認できるため，アジア・オセアニア地域に限定すると GPS スプーフィングについては対策を取ることが見込める．本研究は，GPS を主に置いて検討したことから，今後は，QZSS を含む GNSS を含めて，更なる想定を考えていく必要がある．

また，本研究で取り上げた航法以外に，量子コンパスを利用した新たな航法システムである量子航法が存在する．量子コンパスは，従来の「自己位置推定」を提供するジャイロコンパスのような計測技術と量子技術による正確さを組み合わせた GPS を利用せずに位置計測が可能とされる [62]．量子航法は，イギリス海軍が量子航法システムを潜水艦に搭載し，世界で最初の試験実施に成功している [63]．この成功は，海軍技術における重要な前進を示すと共に様々な海事シナリオにおける船舶の航行能力と運用効率の向上に良い影響を及ぼすとして，世界中が注目されている．

謝辞

本研究の遂行にあたり，指導教官として終始多大なご指導を賜った，情報セキュリティ研究科教授 須崎先生に深謝致します．同研究科教授 土井先生，並びに教授 藤本先生には，本論文の作成にあたり，副査としてご助言を賜りました．そして，広島商船高等専門学校准教授 岸先生，同学校専攻科 坂本氏，同学校 野元氏，並びに株式会社ラック 長谷川氏に本研究の遂行にあたり多大なご助言と実験・評価に協力頂きました．最後に，情報セキュリティ研究科客員教授 松井先生に本研究の遂行にあたり多大なご助言，ご協力頂きました．ここに感謝の意を表します．

参考文献

[1] NSM. 「risiko 2020」. https://nsm.no/getfile.php/131421-1587034764/NSM/Hermans%20undermappe%20med%20bilder/NSM_Risiko_2020_web_0104.pdf, 2020. (visited on Jan. 16, 2024).

[2] Per Håkon Meland, Karin Bernsmed, Egil Wille, Ørnulf Jan Rødseth, and Dag Atle Nesheim. A retrospective analysis of maritime cyber security incidents. 2021.

[3] Anja Menzel and Lisa Otto. Connecting the dots: Implications of the intertwined global challenges to maritime security. *Global Challenges in Maritime Security: An Introduction*, pp. 229–243, 2020.

[4] Above Us Only Stars. Exposing GPS Spoofing in Russia and Syria. https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf, 2019. (visited on Jan. 16, 2024).

[5] Robert Lemos. Coast guard warns shipping firms of maritime cyberattacks, 2019. (visited on Jan. 16, 2024).

[6] Eric Tegle (Forbes JAPAN). 欧州で GPS 妨害が多発，航空機の運航に影響 発信源はロシアか. https://forbesjapan.com/articles/detail/68978, 2024.2.6. (visited on Jan. 16, 2024).

[7] GPS: The Global Positioning System A global public service brought to you by the U.S. government. https://www.gps.gov/. (visited on Jan. 16, 2024).

[8] IMO. SOLAS—Consolidated Edition 2020. *London, UK*, 2020.

[9] IMO MSC. 1/Circ. 1595 e-Navigation Strategy Implementation Plan—Update 1. *London, UK*, 2018.

[10] 海上保安庁, ディファレンシャル GPS の廃止について. https://www.kaiho.mlit.go.jp/10kanku/miyazaki/uminoanzen/kourohyoushiki/deta/dgpsnohaisi190301.pdf, 2019. (visited on Jan. 16, 2024).

[11] IMO MSC. Resolution MSC.428(98) Maritime cyber risk management in Safety Management Systems. *London, UK*, 2017.

[12] IACS. UR E26 "Cyber Resilience of Ships." IACS, 2022.

[13] IACS. UR E27 "Cyber Resilience of On-board Systems and Equipment." IACS, 2022.

[14] 公益財団法人 日本財団ホームページ, 無人運航船プロジェクト「MEGURI2040」. https:

//www.nippon-foundation.or.jp/what/projects/meguri2040, 2020. (visited on Jan. 16, 2024).

[15] 仙田眞之, 須崎有康. GPS ベースの船舶航海システムに対する攻撃と防御. コンピュータセキュリティシンポジウム 2023 論文集, pp. 1293–1300, 2023.

[16] 坂本彩乃, 野元梨乃, 仙田眞之, 岸拓真, 須崎有康, 長谷川長一. 船舶の GPS Spoofing における運航システムへの影響に関する基礎的研究. 暗号と情報セキュリティシンポジウム 2024 論文集, 2024.

[17] 近藤信竹. AIS (自動識別通報装置). Techno marine 日本造船学会誌, Vol. 851, pp. 297–301, 2000.

[18] Marco Balduzzi, Alessandro Pasta, and Kyle Wilhoit. A security evaluation of ais automated identification system. In *Proceedings of the 30th annual computer security applications conference*, pp. 436–445, 2014.

[19] Enricad' Afflisio, Paolo Braca, Peter Willett. Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection. *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 57, No. 4, pp. 2093–2108, 2021.

[20] Wu, Jianjun and Thorne-Large, James and Zhang, Pengfei. Safety first: The risk of over-reliance on technology in navigation. *Journal of Transportation Safety & Security*, Vol. 14, No. 7, pp. 1220–1246, 2022.

[21] Alan G Bole, Alan D Wall, and Andy Norris. *Radar and ARPA manual: radar, AI and target tracking for marine radar users*. Butterworth-Heinemann, 2013.

[22] International Electrotechnical Commission, et al. Maritime navigation and redio-communication equipment and systems, track control systems, operational and performance requirements, methods of testing and required test results. *IEC62065*, pp. 64–72, 2002.

[23] Adam Weintrit. *The electronic chart display and information system (ECDIS): an operational handbook*. CRC Press, 2009.

[24] Boris Svilicic, David Brčić, S Žuškin, and D Kalebić. Raising awareness on cyber security of ECDIS. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 13, No. 1, pp. 231–236, 2019.

[25] Mass Soldal Lund, Odd Sveinung Hareide, and Øyvind Jøsok. An attack on an integrated navigation system. 2018.

[26] 茂在寅男, 小林實. コンパスとジャイロの理論と実際. 海文堂, 1971.

[27] Mohinder S Grewal, Lawrence R Weill, and Angus P Andrews. *Global positioning systems, inertial navigation, and integration*. John Wiley & Sons, 2007.

[28] 松本吉春. 精説地文航法. 成山堂書店, 1997.

[29] 廣野康平. 天文航法の ABC: 天測の基本から観測・計算・測位の実際まで. 成山堂書店, 2020.

[30] 海上保安庁. 「天測暦」等の廃刊について. https://www1.kaiho.mlit.go.jp/KOHO/announce.html. (visited on Jan. 16, 2024).

[31] Greg Tozzi. Toward Automated Celestial Navigation with Deep Learning. https://github.com/gregtozzi/deep_learning_celnav, 2020. (visited on Jan. 16, 2024).

[32] United States. Coast Guard. *Loran-C User Handbook*. Department of Transportation, Coast Guard, 1974.

[33] Walter Blanchard. The genesis of the Decca Navigator system. *The Journal of Navigation*, Vol. 68, No. 2, pp. 219–237, 2015.

[34] J Kasper and C Hutchinson. The Omega navigation system–An overview. *IEEE Communications Society Magazine*, Vol. 16, No. 3, pp. 23–35, 1978.

[35] 海上保安庁. 「慶佐次ロランC局の廃止について」. https://www.kaiho.mlit.go.jp/info/kouhou/h26/k20140801/k140801-1.pdf. (visited on Jan. 16, 2024).

[36] Di Qiu, Dan Boneh, Sherman Lo, and Per Enge. Reliable location-based services from radio navigation systems. *Sensors*, Vol. 10, No. 12, pp. 11369–11389, 2010.

[37] 海上保安庁. 「ロランC」. https://www.kaiho.mlit.go.jp/syoukai/soshiki/toudai/lolanc/index.htm, 2014. (visited on Jan. 16, 2024).

[38] European GNSS Service Centre. What is Galileo. https://www.gsc-europa.eu/galileo/what-is-galileo. (visited on Jan. 16, 2024).

[39] GLONASS. https://glonass-iac.ru/. (visited on Jan. 16, 2024).

[40] Beidou. http://www.beidou.gov.cn/. (visited on Jan. 16, 2024).

[41] NavIC. https://glonass-iac.ru/. (visited on Jan. 16, 2024).

[42] 内閣府宇宙開発戦略推進事務局. みちびきウェブサイト. https://qzss.go.jp/. (visited on Jan. 16, 2024).

[43] 内閣府宇宙開発戦略推進事務局.「信号認証サービス」(みちびきウェブサイト). https://qzss.go.jp/overview/services/sv14_sas.html, 2023. (visited on Jan. 16, 2024).

[44] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*, pp. 75–86, 2011.

[45] Alan Bensky. *Wireless positioning technologies and applications*. Artech House, 2016.

[46] GPS.gov. GPS Standard Positioning Service (SPS) Performance Standard. https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf, 2020. (visited on Jan. 16, 2024).

[47] Jon S Warner and Roger G Johnston. GPS spoofing countermeasures. *Homeland Security Journal*, Vol. 25, No. 2, pp. 19–27, 2003.

[48] Stefan Erker, Steffen Thölert, Johann Furthner, and Michael Meurer. L5–the new gps signal. *Proceedings of IAIN*, pp. 27–30, 2009.

[49] Brian C Barker, John W Betz, John E Clark, Jeffrey T Correia, James T Gillis, Steven Lazar, Kaysi A Rehborn, and John R Straton. Overview of the GPS M code

signal. In *Proceedings of the 2000 National Technical Meeting of the Institute of Navigation*, pp. 542–549, 2000.

[50] Elliott D Kaplan and Christopher Hegarty. *Understanding GPS/GNSS: principles and applications*. Artech house, 2017.

[51] 坂井丈泰. GPS のセキュリティ: 脆弱性とその対策. 電子情報通信学会技術研究報告; 信学技報, Vol. 118, No. 193, pp. 1–6, 2018.

[52] Alan Grant, Paul Williams, Nick Ward, and Sally Basker. GPS jamming and the impact on maritime navigation. *The Journal of Navigation*, Vol. 62, No. 2, pp. 173–187, 2009.

[53] Daniel Medina, Christoph Lass, Emilio Pérez Marcos, Ralf Ziebold, Pau Closas, and Jesús García. On GNSS jamming threat from the maritime navigation perspective. In *2019 22th International Conference on Information Fusion (FUSION)*, pp. 1–7. IEEE, 2019.

[54] Dana, Goward. Mass GPS Spoofing Attack in Black Sea. `https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea`, 2021. (visited on Jan. 16, 2024).

[55] Mark L Psiaki and Todd E Humphreys. Gnss spoofing and detection. *Proceedings of the IEEE*, Vol. 104, No. 6, pp. 1258–1270, 2016.

[56] Dennis M Akos. Who's afraid of the spoofer? gps/gnss spoofing detection via automatic gain control (agc). *NAVIGATION: Journal of the Institute of Navigation*, Vol. 59, No. 4, pp. 281–290, 2012.

[57] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. Pre-despreading authenticity verification for gps l1 c/a signals. *NAVIGATION: Journal of the Institute of Navigation*, Vol. 61, No. 1, pp. 1–11, 2014.

[58] Esteban Garbin Manfredini, Beatrice Motella, and Fabio Dovis. Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests. In *Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, pp. 3100–3106, 2015.

[59] Andriy Konovaltsev, Manuel Cuntz, Christian Haettich, and Michael Meurer. Autonomous spoofing detection and mitigation in a gnss receiver with an adaptive antenna array. In *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, pp. 2937–2948, 2013.

[60] 岸拓真, 濵崎淳, 清田耕司, 坂本彩乃. 船舶における OT 機器を伴うサイバーインシデントへのレスポンスに関する教育プログラムの開発. 第 149 回講演会日本航海学会講演予稿集 11 巻 2 号, pp. 43–46, 2023.10.

[61] IIvan Petrovski and Takuji Ebinuma. Everything you always wanted to know about

GNSS simulators but were afraid to ask. *Inside GNSS September (2010)*, pp. 48–58, 2010.

[62] Imperial College London. Imperial News「Quantum ‘compass’ could allow navigation without relying on satellites」. https://www.imperial.ac.uk/news/188973/quantum-compass-could-allow-navigation-without/, 2018. (visited on Jan. 16, 2024).

[63] Imperial College London. Imperial News「Quantum sensor for a future navigation system tested aboard Royal Navy ship」. https://www.imperial.ac.uk/news/245114/quantum-sensor-future-navigation-system-tested/, 2023. (visited on Jan. 16, 2024).