

高周波受信機では背景雑音の中から信号を「聞く」ことすら困難である¹³。この信号の弱さは、比較的低電力の衛星送信機で全地球をカバーすることを可能にする一方で、地上からのわずかな出力の干渉波によっても容易に影響を受けてしまうという、いわば諸刃の剣と言える。

干渉の種類とそのメカニズム (Types of Interference and Their Mechanisms)

GNSS信号への干渉は、その発生原因や意図の有無によって、偶發的干渉と意図的干渉に大別される。

偶發的干渉 (Unintentional Interference):

偶發的干渉は、悪意なく発生するもので、主に環境要因と他の電子機器からの不要電波が原因となる。

- 環境要因:
 - 大気遅延: GNSS信号は地球の大気圏を通過する際に遅延を受ける。電離層（高度約50～1000km）ではプラズマの影響で、対流圏（高度約10kmまで）では水蒸気や気圧の影響で信号伝播速度が変化し、測位誤差の原因となる³²。特に電離層の擾乱（太陽フレアや磁気嵐に伴うもの）は深刻な影響を及ぼすことがある¹。
 - マルチパス: 信号が建物、地形、樹木などの障害物で反射し、直接波と反射波が干渉したり、遅れて到達した反射波を受信機が誤って直接波として処理したりすることで測位誤差が生じる¹。特に高層ビルが密集する「都市峡谷」と呼ばれる環境では、この影響が顕著である³⁴。
 - 信号遮蔽: 樹木が密集した場所や屋内などでは、GNSS信号が遮蔽され、受信強度が低下したり、信号が完全に途絶したりすることがある¹。
- 電磁両立性 (EMC) の問題:

現代社会は多種多様な電子機器で溢れおり、これらの機器から放射される電波がGNSS信号に干渉することがある。これらはスペクトル規制によりGNSS帯域内での放射は厳しく制限されているものの、帯域外（Out-of-Band）の強力な信号や、その高調波・相互変調積がGNSS帯域内（In-Band）に影響を及ぼすことがある³¹。具体的には、テレビ・ラジオ放送塔、高圧送電線、レーダーシステム、産業機械、さらには家庭内の電子レンジや無線LANルータ、ワイヤレスカメラ、LED照明、太陽光発電システムのパワーコンディショナなども干渉源となりうる¹³。例えば、日本では過去に工事現場のクレーンに設置されたワイヤレスカメラ³⁵や、不適切な配線がされたテレビ受信用ケーブル³⁵がGNSS受信に障害を引き起こした事例が報告されている。

意図的干渉 (Intentional Interference):

意図的干渉は、GNSSの利用を妨害したり、欺いたりすることを目的として行われる。

- ジャミング (Jamming):

ジャミングは、GNSS信号が使用する周波数帯域に、意図的に強力な妨害電波やノイズを放射し、受信機が正規の衛星信号を正常に受信・追尾・復調することを不可能にする行為である⁸。ジャマー（妨害装置）には、特定の周波数のみを狙う狭帯域ジャマー、広範囲の周波数に影響を与える広帯域ジャマー、周波数を掃引するチャーブジャマー、断続的に妨害波を出すパルスジャマーなど、様々な種類が存在する¹³。これらのジャミングにより、受信機における信号対雑音比（SNRまたはC/N0）が著しく低下し、最悪の場合、測位が完全に不可能になったり、追尾ループがロックを失ったりする¹³。
- スピーフィング (Spoofing):

スピーフィングは、正規のGNSS衛星信号を模倣した偽の信号を送信し、受信機を欺いて誤った位置情報や時刻情報を計算させる、より高度で悪質な攻撃である⁸。攻撃手法は、単純に記録したGNSS信号を再放送するものから、受信機の追尾ループと同期を取り、徐々に偽信号の強度を上げて正規信号から引き離し、受信機を完全に制御下に置く「キャリーオフ攻撃（carry-off attack）」のような洗練されたものまで多岐にわたる²⁶。スピーフィングの最大の問題点は、受信機が偽のPNT情報を正しいものとして処理してしまうため、攻撃を受けていることに利用者が気づきにくく、結果として誤った判断や行動を誘発するリスクが高いことである¹⁴。

ジャミングがGNSSの「可用性」を奪うサービス妨害であるのに対し、スピーフィングはPNT情報の「信頼性（インテグリティ）」を根本から揺るがす欺瞞行為であり、検知されなければより深刻な事態を引き起こす可能性がある。この脅威の質の変化は、単なるノイズ除去に留まらない、信号の真正性を検証する認証技術の重要性を浮き彫りにしている。

GNSS測位精度および可用性への影響 (Impact on GNSS Positioning Accuracy and Availability)

GNSS信号への干渉は、測位精度、可用性、信頼性（インテグリティ）の全てに悪影響を及ぼす。

- 測位精度の低下: 干渉によりC/N0が劣化すると、測位計算に用いられる擬似距離測定値のノイズが増加し、測位誤差が数メートルから数百メートル、あるいはそれ以上に増大する¹³。
- 可用性の低下: 強力な干渉下では、受信機は衛星信号の追尾を維持できなくなり、測位解が得られなくなる（測位不能）。また、高精度なRTK（Real Time Kinematic）測位モードから、より精度の低い単独測位モードへのフォールバックを余儀なくされることもある¹³。これにより、高精度測位を前提とするアプリケーション（例えば、ド

ローンの自律飛行や精密農業機械の自動操舵)は機能不全に陥る可能性がある¹³。

- **信頼性(インテグリティ)の喪失:**特にスプーフィング攻撃の場合、受信機は誤った位置や時刻を正しい情報として出し続けるため、PNT情報の信頼性が著しく損なわれる¹⁴。これは、利用者が誤情報に基づいて危険な判断を下すリスクを高める。例えば、航空機が誤った飛行経路を辿ったり、船舶が危険水域に進入したりする事態が想定される。

干渉はまた、受信機が最初の測位解を得るまでの時間（TTFF: Time To First Fix）を増大させ、特にバッテリー駆動のデバイスでは消費電力の増加にも繋がる³⁶。

3. GNSS信号干渉の歴史的経緯と主要事例 (Historical Trajectory and Major Incidents of GNSS Signal Interference)

GNSS信号干渉の歴史は、初期の偶発的なものから、近年ではより意図的かつ組織的な活動へとその様相を変えてきている。特に紛争地域や地政学的に緊張が高い地域では、GNSS干渉が常態化しつつある。

世界的な干渉事例の変遷と顕著なインシデント (Evolution of Global Interference Incidents and Notable Events)

GNSS干渉の報告は年々増加しており、その手口も巧妙化している。以下に主要なインシデントと傾向を示す。

- **アゼルバイジャン航空機墜落事故 (2024年末、グロズヌイ):** 2024年末、アゼルバイジャン航空のエンブラエルE190型機がロシア連邦チェチェン共和国の首都グロズヌイへの着陸進入中に墜落した事故は、GPS妨害が要因の一つとして調査されている。ロシア当局は当時、ウクライナのドローン攻撃に対応するためGPS妨害を行っていたことを認めている⁶⁹。一部報道では、ロシア側の対空ミサイルシステムも干渉の影響を受け、民間航空機を正しく識別できなかった可能性が指摘されており⁶⁹、GNSS干渉が航空安全に及ぼす深刻な影響を改めて浮き彫りにした¹⁹。
- **中東・北アフリカ (MENA) 地域における広範な干渉:** 2021年には、MENA地域および隣接諸国で586件のGNSS/GPSジャミングまたはその疑いのある事象が15のオペレーターから報告され、さらに38のオペレーターからは46,936件のGPS信号喪失イベントが記録された⁷⁰。特にトルコのアンカラFIR (飛行情報区) およびイスタンブルFIRでの報告が際立っており、この地域におけるGNSS干渉の深刻さを示している⁷⁰。
- **バルト海地域における干渉:** 近年、バルト海地域、特にロシアの飛び地であるカリーニングラード周辺から強力なジャミングが発生し、広範囲（半径200海里以上）の航空機や船舶の航行に影響を与えていている³⁸。2024年6月から11月にかけてグディニャ海洋大学とGPSPATRONが実施した調査では、バルト海沿岸で合計84時間のGNSS干渉が検出され、その多くはジャミングによるものであった。移動する船舶からのジャミングの可能性も指摘されている⁷²。
- **ロシア・ウクライナ紛争に伴う干渉の激化:** ロシアによるウクライナ侵攻以降、両国および周辺地域では、軍事作戦の一環としてGPSジャミングやスプーフィングが日常的に使用されている¹⁹。これは、敵の航法システムを無力化し、自軍の行動を秘匿する目的で行われていると考えられる³⁷。
- **スプーフィング事例の増加と巧妙化:**
 - 2011年、イランが米国のドローンをスプーフィングによって捕獲したとされる事例⁵²。
 - 2017年、黒海で多数の船舶が実際の位置とは異なる場所にいると誤認させられる大規模スプーフィングが発生⁵²。
 - 2020年、中国沿岸の20箇所以上で船舶が円を描くように航行しているように見せかける「サークルスプーフィング」が報告された⁵²。これらの事例は、スプーフィング技術が高度化し、広範囲に影響を及ぼしうることを示している。
- **航空分野でのインシデント急増:** OPSGROUPの報告によると、2024年の夏には1日あたり平均1500便がスプーフィングの影響を受けており、これは2024年第1四半期/第2四半期の約300便から大幅な増加である⁷⁵。また、IATA.orgの報告では、2021年8月から2024年6月までの間に1840万便のフライトで58万件以上のGPS信号喪失が記録されている⁷⁶。これらの数字は、航空分野におけるGNSS干渉が常態化しつつあることを示している。

以下の表に、主要なGNSS干渉インシデントの年表を示す。

表1: 主要なGNSS干渉インシデント年表

年代	地域/場所	干渉タイプ	推定原因/主体	影響を受けた分野	主要な影響	典拠
2011年	イラン	スプーフィン	イラン軍	軍事（ドロー	米国ドローン	52

		グ		ン)	の捕獲	
2017年	黒海	スプーフィング	不明（国家主体が疑われる）	海事	数百隻の船舶が誤った位置情報を表示	52
2020年12月	日本・小松空港周辺	偶発的干渉（広帯域ノイズ）	工事現場クレーンのワイヤレスカメラ	航空	航空機のGPS受信障害、運航遅延・欠航	35
2020年	中国沿岸	スプーフィング（サークルスプーフィング）	不明（国家主体が疑われる）	海事	20箇所以上で船舶が実際とは異なる円運動を表示	52
2021年	中東・北アフリカ（MENA）地域	ジャミング、信号喪失	不明（紛争、軍事活動に関連する可能性）	航空	586件のジャミング報告、46,936件の信号喪失イベント	70
2022年～継続	ロシア・ウクライナおよび周辺地域	ジャミング、スプーフィング	ロシア軍、ウクライナ軍	軍事、航空、海事、民生	広範囲なPNT情報の信頼性低下、航法障害	37
2024年	バルト海地域（特にカリーニングラード周辺）	ジャミング	ロシア（カリーニングラードからと推定）	航空、海事	広範囲なGPS信号妨害、航空機のルート変更、船舶の航行困難	38
2024年末	ロシア・グロズヌイ	ジャミング（スプーフィングの可能性も）	ロシア軍	航空	アゼルバイジャン航空機墜落事故の一因と調査中	19
2024年～継続	複数地域（特に紛争地域周辺）	スプーフィング	不明（国家主体、非国家主体を含む可能性）	航空	1日あたり最大1500便が影響、航空機の誤誘導リスク	41

日本国内における干渉事例とその教訓 (Interference Incidents within Japan and Lessons Learned)

日本国内においても、GNSS信号への干渉事例は発生しており、その多くは偶発的なものであるが、重要な教訓を含んでいる。

- 小松空港でのGPS受信障害（2020年12月）**: 石川県の小松空港において、駐機中の航空機がGPS信号を受信できなくなり、運航に遅延や欠航が発生した。調査の結果、空港から約3.8km離れた大規模工事現場で使用されていたクレーンのアーム先端に取り付けられたワイヤレスカメラのトランスマッターから発射された広帯域の電波が原因と特定された³⁵。このカメラはクレーン運転手が個人的に設置したものであり、GPSだけでなく、電波天文、携帯電話、気象レーダーソンデなど、広範な周波数帯に影響を及ぼす可能性があった。当該カメラの撤去により干渉は解消された。この事例は、意図しない電波源であっても、航空機の安全運航に不可欠なGNSSシステムに深刻な影響を与えることを示している。
- SUPERBIRD衛星音楽放送の受信障害**: 2019年頃から、SUPERBIRD衛星を利用したCS音楽放送において断続的な受信障害が発生した。広範な調査の結果、特定のメーカーの車載レーダー探知機からのスプリアス発射（規定外の不要な電波）が原因であることが判明した³⁵。レーダー探知機の局部発振器からの漏洩電波がCS受信用パラボラアンテナに入り込み、衛星からの微弱な信号をマスキングしていた。この事例は、民生用電子機器の設計不備や品質管理の問題が、広範囲の衛星通信サービスに影響を及ぼす可能性を示唆している。

これらの国内事例は、紛争地域のような意図的な妨害がない環境下においても、偶発的な干渉源によって重要システムが脆弱であることを示している。これは、電磁両立性（EMC）に関する国内規制の遵守徹底、不法無線局の監視強化、そして干渉源の迅速な特定と除去を行うための体制整備の重要性を強調している。軍事的脅威とは独立して、国内にお

ける電波利用環境の健全性を維持するための継続的な努力が不可欠である。

特定分野における影響分析 (Analysis of Impacts on Specific Sectors)

GNSS干渉は、測位・航法・時刻同期に依存するあらゆる分野に影響を及ぼす。

- **航空 (Aviation):** 航空分野では、航法システム（RNAV、RNP）、着陸支援システム（LPVアプローチ等）、監視システム（ADS-B）、通信システム（CPDLC）、そして地上接近警報装置（EGPWS/TAWS）などがGNSSに依存している⁷⁷。干渉が発生すると、これらのシステムの機能が低下または喪失し、航空機の位置情報が不正確になったり、EGPWSが誤作動して不必要的急上昇操作を誘発したりする危険性がある⁵¹。実際、2024年末のアゼルバイジャン航空機墜落事故では、GPS妨害が状況を悪化させた可能性が指摘されている⁶⁹。また、スプーフィングによって航空機が誤った経路に誘導されるリスクも存在する⁵¹。航空管制（ATC）においても、ADS-Bからの誤った位置情報により、航空交通管理に混乱が生じる可能性がある⁷⁹。
- **海事 (Maritime):** 船舶の航行において、GNSSは安全かつ効率的な運航に不可欠である。ジャミングやスプーフィングは、船舶を正しい航路から逸脱させ、座礁や衝突のリスクを高める²⁷。特に、自動船舶識別装置（AIS）はGNSS測位情報に依存しているため、スプーフィングによって船舶の位置が偽装され、密輸や違法操業などの不正行為に悪用されるケースも報告されている²⁷。バルト海や東地中海などの高リスク海域では、GNSS干渉が常態化しつつあり、代替航法手段を持たない船舶は深刻な危険に晒されている³⁸。
- **重要インフラ (Critical Infrastructure):**
 - **電力網 (Power Grids):** 電力系統の安定運用には、広域に分散した観測点（PMU: 位相計測装置など）からのデータをミリ秒以下の精度で同期させる必要があり、その時刻源としてGNSSが広く利用されている³。GNSS時刻同期が失われると、系統の監視・制御が困難になり、最悪の場合、大規模停電を引き起こす可能性がある²³。2016年に発生したGPSの時刻情報が13マイクロ秒ずれたインシデントでは、通信網や電力網を含む精密な時刻同期を必要とするシステムが広範囲にわたり影響を受けた⁹。
 - **金融 (Finance):** 金融取引においては、取引の順序性やトレーサビリティを確保するため、高精度な時刻同期が不可欠であり、多くの金融機関がGNSSを時刻源として利用している³。スプーフィング攻撃によるタイムスタンプの改竄は、取引の正当性を損ない、市場に混乱をもたらす可能性がある²³。
 - **通信 (Telecommunications):** 携帯電話基地局やデジタル放送網など、多くの通信システムが周波数・位相同期のためにGNSS時刻を利用している³。干渉による時刻同期の喪失は、通信品質の低下やサービス停止に繋がる。
- **その他分野 (Other Sectors):**
 - **精密農業:** 農機の自動操舵、可変施肥・散布、収量マッピングなど、精密農業の多くの側面で高精度GNSSが利用されている⁴³。干渉は作業精度を低下させ、収量減や資源の無駄遣いを引き起こす。
 - **自動運転・ドローン:** 自動運転車やドローンの安全な自律走行・飛行には、正確で信頼性の高いPNT情報が不可欠である¹³。干渉、特にスプーフィングは、車両の誤誘導やドローンの墜落・逸走といった重大事故に直結する。
 - **建設ICT:** ICT施工における建機の自動制御や測量にもGNSSが活用されており、干渉は作業効率の低下や施工不良の原因となる。

これらの多様な分野への影響は、GNSS干渉が単なる測位の問題ではなく、広範な経済・安全保障上の脅威であることを示している。特に、金融や通信分野におけるGNSS時刻同期への依存度は、測位への依存度ほど一般に認識されていない場合が多く、潜在的な脆弱性となっている。したがって、GNSSの脆弱性評価とレジリエンス確保においては、測位情報だけでなく時刻情報の重要性も十分に考慮する必要がある。

4. GNSS信号干渉への対策技術動向 (Trends in Mitigation Technologies for GNSS Signal Interference)

GNSS信号干渉の脅威増大に対応するため、受信機レベル、アンテナレベル、そしてシステム全体レベルでの様々な対策技術が研究開発され、実用化が進められている。

受信機ベースの耐干渉技術 (Receiver-based Anti-interference Technologies)

受信機内部の信号処理によって干渉の影響を軽減する技術は、対策の第一線として重要である。

- **適応フィルタリング (Adaptive Filtering):** 受信信号の特性に応じてフィルタのパラメータを動的に調整し、干渉波を選択的に除去する技術群である。
 - **ノックフィルタ:** 特定の狭帯域干渉（例えば、連続波干渉）を効果的に除去する。干渉波の周波数を検出し、その周波数成分のみを鋭く減衰させるフィルタを適応的に形成する¹³。LMS（Least Mean Squares）アルゴリズムやRLS（Recursive Least Squares）アルゴリズムを用いた適応型FIR（Finite Impulse Response）ノック

チフィルタなどが提案されている⁸⁸。

- **パルスブランкиング:** 短時間の強力なパルス性干渉を検出し、その期間の信号を一時的に無効化（ブランкиング）することで影響を軽減する¹³。
 - **広帯域干渉低減:** チャーブジャマーのような周波数が変動する広帯域干渉に対しては、より高度な適応フィルタリング技術が用いられる¹³。
 - **FFTベースの干渉除去:** 高速フーリエ変換（FFT）を用いて信号を周波数領域に変換し、干渉成分を特定・除去した後に時間領域に戻す手法も、特に強力な干渉除去方法として提案されている⁹¹。
 - **ウェーブレット変換:** 信号の時間–周波数解析に優れ、パルス性干渉や狭帯域干渉など、多様な干渉の検知・除去に応用されている⁹³。
 - **時間–周波数領域処理:** STFT (Short-Time Fourier Transform)などの時間–周波数表現を利用し、干渉信号を2次元平面上で分離・除去するアプローチも研究されている⁹⁵。
 - **カルマンフィルタ:** 主にGNSSと他のセンサー（INS等）を統合する際に用いられるが、観測ノイズの特性を適応的に推定することで、干渉による測位誤差の増大を抑制する効果も期待される⁹⁰。
- **自律的健全性監視 (Autonomous Integrity Monitoring):**
受信機自身が受信信号の品質や測位解の一貫性を監視し、異常を検知・警告・排除する機能である。
- **RAIM (Receiver Autonomous Integrity Monitoring):** 複数の衛星からの擬似距離測定値の冗長性を利用して、統計的な手法（最小二乗残差法など）に基づいて、いずれかの衛星信号に大きな誤差（障害）が含まれていないかを検査する⁹⁷。障害が検知された場合、その衛星を測位計算から除外するFDE (Fault Detection and Exclusion) 機能を持つものもある。
 - **ARAIM (Advanced RAIM):** マルチGNSSコンステレーション環境での利用を想定し、より高度な障害検知・排除能力を持つRAIMの進化版である。地上監視網からの衛星健全性情報（ISM: Integrity Support Message）も活用する⁹⁷。航空分野での利用が先行しているが、海事、UAS、鉄道など他分野への応用も検討されている⁹⁷。
- **信号認証 (Signal Authentication):**
スプーフィング攻撃に対抗するため、受信したGNSS信号が正規の衛星から送信されたものであるか、また航法メッセージが改竄されていないかを検証する技術である。
- **OSNMA (Open Service Navigation Message Authentication):** Galileoが提供するオープンサービス向けの航法メッセージ認証。秘密鍵と公開鍵を用いたデジタル署名技術に基づき、航法データの真正性を保証する⁵⁵。TESLA (Timed Efficient Stream Loss-Tolerant Authentication) プロトコルの変種を利用して、遅延鍵開示によって真正性を担保する⁵⁵。
 - **Chimera:** GPS近代化信号（L1C等）に導入が計画されている信号認証技術。航法メッセージ認証に加え、拡散符号の認証も行うことで、より強力なスプーフィング対策を目指す⁵⁵。
 - **QZNMA (QZSS Navigation Message Authentication):** 日本の準天頂衛星システム「みちびき」（QZSS）が2024年4月から提供を開始した航法メッセージ認証サービス。デジタル署名と公開鍵暗号方式を利用して、受信機側で航法メッセージの改竄有無を検証可能とする⁶⁰。

受信機ベースの対策技術は、ジャミングのようなノイズ除去から、スプーフィングのような巧妙な欺瞞行為への対抗へと進化しており、これは脅威の性質変化を反映している。初期の対策は既知の干渉パターン（例えば連続波干渉）に対するフィルタリングが主であったが¹³、RAIM/ARAIMは衛星信号の冗長性に基づく信頼性評価を加えた⁹⁷。そして、正規信号を模倣するスプーフィングの台頭は、信号源とデータ内容の暗号論的な認証（OSNMA、Chimera、QZNMAなど）という、より高度な防御策を必要とさせている⁵⁵。

アンテナベースの耐干渉技術 (Antenna-based Anti-interference Technologies)

アンテナ自体に干渉波を抑制する機能を持たせることで、受信機の前段で干渉の影響を軽減する技術である。

- **CRPA (Controlled Reception Pattern Antenna) / アレイアンテナ:** 複数のアンテナ素子を配列し、各素子で受信した信号の位相や振幅を適応的に制御することで、アンテナの指向性パターンを動的に変化させる⁵。
 - **ヌルステアリング:** 干渉波の到来方向に受信感度の低いヌル（零点）を形成し、干渉波の受信を抑圧する⁵。
 - **ビームフォーミング:** 目的とするGNSS衛星の方向に受信感度の高いビームを形成し、衛星信号の受信電力を最大化する⁵。CRPAは特に軍事分野や重要インフラ防護など、高度な耐干渉性が求められる用途で有効であるが、一般に大型で高価になる傾向がある⁵。
- **チョークリングアンテナ (Choke Ring Antenna):** アンテナのグラウンドプレーンに同心円状の溝（チョークリング）を設けることで、地面や周辺構造物からの反射波（マルチパス波）を効果的に抑制する³³。主に固定局（電子基準点など）で高精度測位のために用いられる。
- **マルチパス軽減アンテナ設計:** アンテナ素子の形状や配置、材質などを工夫することで、マルチパスの影響を低減するように設計されたアンテナ³⁴。デュアル周波数CMC（Code-Minus-Carrier）法などの技術と組み合わせて評

価されることもある¹¹⁵。

CRPAのような高度なアンテナ技術は非常に効果的である一方、そのサイズ、コスト、複雑性の面で制約があり、全てのユーザーセグメント、特に民生用デバイスへの広範な搭載は現状では限定的である⁵。このため、マスマーケット向けの小型かつ低コストで実用的な耐干渉アンテナソリューションの開発が求められている。

システムレベルでの耐性強化と代替PNT技術 (System-level Resilience Enhancement and Alternative PNT Technologies)

単一のGNSSシステムや技術に依存するのではなく、複数のシステムや技術を組み合わせることで、全体としてのPNT情報の信頼性と頑健性を高めるアプローチである。

- **マルチGNSS/マルチ周波数受信:** 複数のGNSSコンステレーション (GPS、GLONASS、Galileo、BeiDou、QZSS等) および複数の周波数帯 (L1、L2、L5等) の信号を同時に利用することで、可視衛星数の増加による測位ジオメトリの改善、周波数ごとの干渉特性の違いを利用した耐性向上、一部のシステムや周波数帯が利用不能になった場合の冗長性確保などが期待できる¹⁴。ただし、受信帯域幅の増大は新たな干渉対策の課題も生む³¹。
- **LEO-PNT (Low Earth Orbit PNT):** 従来のMEO (Medium Earth Orbit、中軌道) GNSS衛星 (高度約2万km) よりも低い軌道 (数百~数千km) を周回する衛星コンステレーションを利用したPNTシステム⁴。衛星と受信機間の距離が近いため信号強度が高く、ジャミングに対する耐性が向上する¹²¹。また、衛星の動きが速いためジオメトリ変化が大きく、RTKやPPPの収束時間短縮にも寄与する¹³¹。CバンドなどLバンド以外の周波数帯を利用することで周波数ダイバーシティも確保できる¹²¹。StarlinkやIridium STLなどが代表例として挙げられる¹²¹。
- **eLoran (Enhanced Loran):** 地上系の中波帯電波航法システムであるLoran-Cを近代化したもの。GNSSとは全く異なる物理層を利用するため、GNSSが利用不能な場合の強力なバックアップとして期待されている²⁵。広域をカバーでき、信号強度も比較的強い。
- **慣性航法システム (INS) / センサーフュージョン:** 加速度センサーやジャイロスコープからなるIMU (Inertial Measurement Unit) は、外部からの信号に依存せずに自身の動きを積分して位置や姿勢を推定する¹⁹。ただし時間とともに誤差が累積するため、GNSSやオドメータ (車輪速センサー) 、カメラを用いたVisual SLAM (Simultaneous Localization and Mapping) /VIO (Visual-Inertial Odometry) 、LiDAR SLAMなど、他のセンサー情報と統合 (センサーフュージョン) することで、GNSSが利用できない環境下でもPNT情報を補完・維持する⁹⁰。
- **量子センサー (Quantum Sensors):** 量子力学的な現象を利用した超高感度センサー。原子時計 (チップスケール原子時計 (CSAC) を含む) による時刻ホールドオーバー¹³⁷、原子干渉計を用いた慣性センサー (加速度計、ジャイロスコープ) 、量子磁力計、重力計・重力勾配計などが研究されており、従来のセンサーを凌駕する精度や長期安定性が期待される¹³¹。GNSSが利用できない環境での自律航法への応用が期待される。
- **Signals of Opportunity (SoOp):** Wi-Fi、Bluetooth、携帯電話基地局の電波、FM/AMラジオ放送波、地上デジタルテレビ放送波など、測位専用ではない既存の様々な無線信号を「機会信号」として捉え、それらを利用して測位を行う技術³⁴。特に都市部などGNSSの受信が困難な環境での補完技術として注目されている。

これらの代替PNT技術の多様化は、GNSS特有の干渉に対するレジリエンスを高める一方で、システム間の統合、標準化、そして新たな脆弱性の出現といった新たな複雑性をもたらす可能性も秘めている。「システム・オブ・システムズ」としてPNTを捉え、アーキテクチャ全体としての堅牢性を設計していく必要がある。

AI・機械学習を活用した先進的干渉検知・軽減技術 (Advanced Interference Detection and Mitigation using AI/ML)

人工知能 (AI) および機械学習 (ML) 技術は、GNSS干渉の検知、分類、軽減において新たな可能性を拓いている。

- **干渉パターンの学習と識別:** 大量のGNSS信号データと干渉データを学習させることで、既知の干渉だけでなく、未知の、あるいは巧妙に偽装された干渉パターンを識別する能力を獲得することが期待される²⁶。深層学習ネットワークモデルを用いて、受信信号のスペクトログラムなどから干渉の種類を自動分類し、最適な干渉軽減手法を選択する研究が進められている⁴⁵。
- **異常検知:** 時系列データとしてGNSS観測値を捉え、通常とは異なる振る舞い (例えば、C/N0の急激な変動、測位解の飛びなど) を異常として検知する。LSTM (Long Short-Term Memory) ネットワークなどが応用されている⁶⁵。
- **データ圧縮と特徴抽出:** VAE (Variational Autoencoder) のような手法を用いて、GNSS信号から干渉種別、信号強度、帯域幅、干渉源までの距離といった本質的な特徴を抽出し、効率的なデータ圧縮と伝送を可能にする研究もある¹⁴¹。

AI/MLの活用は、従来のプログラムベースの対策では対応が難しかった未知の脅威や動的に変化する干渉環境への適応能力向上に繋がる。しかし、その性能は学習データの質と量に大きく依存し⁶⁵、特に稀な攻撃パターンや新しいタイプの干渉に対する汎化性能の確保が課題となる。また、AIの判断根拠の透明性 (説明可能性) も、特に安全性が重視され

る分野では重要となる。

以下の表に、主要なGNSS干渉対策技術の比較評価を示す。

表2: GNSS干渉対策技術の比較評価

技術カテゴリ	具体技術	動作原理	主な対象干渉	長所	短所/課題	代表的な製品/研究例	典拠
受信機ベース	適応ノッチフィルタ	特定周波数の狭帯域干渉を適応的に除去	狭帯域ジャミング(CW等)	実装容易性、低コスト	広帯域干渉には向き	Septentrio AIM+ ¹³ , NovAtel ANF ⁸⁹	13
	パルスブランディング	短時間パルス性干渉を時間領域で除去	パルスジャミング	高速応答	連続的な干渉には向き	Septentrio AIM+ ¹³	13
	RAIM/ARAIM	衛星信号の冗長性を用いた整合性チェック	衛星故障、一部のマルチパス/RFI	受信機単独でインテグリティ確保	多数の衛星が必要、計算負荷	航空用受信機 ⁹⁷	97
	信号認証(OSNMA, Chimera, QZNMA)	暗号技術による航法メッセージ等の真正性検証	スプーフィング	高いスプーフィング耐性	鍵管理、システム全体の対応が必要	Galileo OSNMA ⁵⁵ , QZSS QZNMA ⁶⁰	55
アンテナベース	CRPA/アレイアンテナ	複数素子アンテナで指向性を制御し干渉を抑圧	広範なジャミング、一部スプーフィング	高い干渉抑圧能力	高コスト、大型、複雑	GAJT (NovAtel) ⁴⁷ , 軍事用アンテナ	5
	チョークリングアンテナ	地面反射波(マルチパス)を物理的に抑制	マルチパス	高いマルチパス除去性能	大型、固定局向け	測量用基準局アンテナ ¹¹³	113
システムレベル/代替PNT	マルチGNSS/マルチ周波数	複数システム・周波数の利用による冗長化	システム障害、一部干渉	可用性・堅牢性向上	受信機複雑化、コスト増	最新の業務用・民生用受信機	14
	LEO-PNT	低軌道衛星によるPNT情報提供	GNSSの弱点補完(信号強度、ジオメトリ)	高信号強度、対ジャミング性向上	システム構築コスト、軌道安定性	Starlink ¹²⁶ , Iridium STL ¹²⁸	121
	eLoran	地上系電波による広域PNT	GNSS障害時のバックアップ	GNSSと異なる干渉特性	カバレッジ限定、インフラ整備	UrsaNav ⁸⁴	25
	INS/センサーフュージョン	自律センサーとGNSS等を統合	GNSS途絶時のPNT維持	GNSS非依存性(短時間)	誤差累積、初期アライメント	航空機FMS ⁷⁷ , 自動運転システム	51
	量子センサー	量子現象を利用した超高精度PNT	未知の脅威への潜在的耐性	超高精度、長期安定性	技術成熟度、コスト、サイズ	研究開発段階 ¹³⁹	139
AI/ML活用	干渉検知・分類・軽減	機械学習による干渉パ	未知・適応型干渉	新規脅威への適応性	学習データ依存、説明	研究開発段階 ⁴⁵	45

Based Augmentation System) 互換の補強信号であり、サブメータ級の測位精度向上とともに、衛星の健全性に関する情報（インテグリティ情報）を提供する⁷。これにより、利用者は測位結果の信頼性を評価し、安全な運用に役立てることができる。

QZSSは、単に測位衛星の数を増やすだけでなく、CLAS/MADOCA-PPPによる精度向上と異常検知、QZNMAによるスプーフィング対策、公共専用信号による高セキュリティ確保、SAIFによるインテグリティ情報提供といった多層的なサービスを通じて、日本のPNTレジリエンス戦略の中核を担っている。これは、多様な脅威に対応し、利用者のニーズに応じた信頼性の高いPNT情報を提供するための国家戦略の表れと言える。

国内研究機関・大学・企業の最新研究開発動向 (Latest R&D Trends from Domestic Research Institutions, Universities, and Companies)

日本のGNSS干渉対策は、政府主導の取り組みに加え、研究機関、大学、民間企業における活発な研究開発によって支えられている。

- **情報通信研究機構 (NICT):** 日本標準時の生成・供給機関として高精度な時刻同期技術を開発するとともに、太陽フレアや磁気嵐といった宇宙天気現象が電離層に与える影響を監視・予測し、GNSS信号伝播への影響評価や警報配信を行っている³³。高分解能TEC (Total Electron Content) 観測網を用いた電離層擾乱の研究は、測位精度向上に不可欠である¹⁷¹。
- **宇宙航空研究開発機構 (JAXA):** QZSSの開発・運用に深く関与し、衛星本体や搭載機器の研究開発を行っている。近年では、MetCom社との共創イニシアチブにおいて、地上基地局の衛星信号受信アンテナにJAXAが開発中のアレイアンテナ技術を組み込むことで、耐干渉性と安全性を向上させる研究を進めている¹¹⁰。また、航空安全インベーションハブなどを通じて、複数のアンテナ素子で受信したGNSS信号を合成し干渉影響を低減する技術など、耐障害高信頼性航法技術の研究も行っている¹¹²。
- **産業技術総合研究所 (AIST):** GNSS受信機の測位アルゴリズムの高精度化、ロバスト化に関する研究を推進している。特に、マルチパス環境下での搬送波位相測位における整数値不定性決定問題や、GNSS受信機ソフトウェアの干渉下での挙動の不確かさの定量化など、基礎的かつ重要な課題に取り組んでいる⁶³。
- **大学における研究:** 各大学の研究室においても、GNSS干渉の検知・除去アルゴリズム、AI/MLの応用、代替測位技術など、多岐にわたる研究が行われている。例えば、深層学習を用いたインテリジェントな干渉軽減手法の研究⁴⁵や、低コストSDR (Software Defined Radio) を用いた空間ダイバーシティによる干渉軽減技術の研究¹⁴³などが報告されている。文部科学省の事業として、衛星測位技術分野の人材育成プログラムも実施されており、大学と企業が連携して干渉・欺瞞信号に関する研究開発や実証実験が行われている¹⁷⁹。
- **国内企業（古野電気、日本無線、トプコン/ソキア等）の耐干渉受信機・アンテナ技術:**
 - **古野電気:** アクティブアンチジャミング機能を搭載したマルチGNSS受信チップ・モジュールを開発・提供しており、特に狭帯域ノイズやジャミング信号の検知・除去に効果を發揮している¹¹⁸。同社のタイミング用マルチGNSS受信機は、ジャミング環境下でも高精度な1PPS信号を出力し続ける性能が示されている¹¹⁹。
 - **日本無線 (JRC):** マルチGNSSに対応し、スプーフィングやジャミングの検知機能を備えた高精度GNSSコンパス「JLR-41」などを製品化している¹²⁰。
 - **トプコン/ソキア:** 同社のGNSS受信機「GRX5」は、アンチジャミング・アンチスプーフィング機能を搭載している¹⁸¹。また、トプコンは適応型ノッチフィルタを用いたGNSS信号干渉軽減方法に関する特許も出願している⁸⁹。
 - **その他、Septentrio社（ベルギーの企業だが日本市場でも活動）の製品も、適応型ノッチフィルタリング、パルスランギング、広帯域干渉低減といった独自の干渉緩和技術（AIM+）を搭載している¹³。**

日本におけるGNSS干渉対策は、内閣府主導のQZSSプロジェクトを核としつつ、総務省、国土交通省、防衛省といった関係省庁がそれぞれの所管分野で政策を推進し、NICT、JAXA、AISTといった国立研究開発法人が専門的な研究開発を担い、大学が基礎研究と人材育成を、そして民間企業が具体的な製品・技術開発を行うという、産学官が連携した「オールジャパン」体制で進められている。この包括的なアプローチは、宇宙セグメントからユーザーセグメントに至るエンドツーエンドでのPNTレジリエンス構築と、国内技術基盤の強化を目指すものである。

6. GNSS信号干渉問題に関する国際的動向と連携 (International Trends and Cooperation on GNSS Signal Interference)

GNSS信号干渉は国境を越える問題であり、その対策には国際的な協調が不可欠である。主要国・地域は独自のPNT戦略を進める一方、国際機関を通じた協力も模索されている。

主要国・地域（米国、欧州、ロシア、中国等）の政策と戦略 (Policies and Strategies of Major Countries/Regions):

US, EU, Russia, China, etc.)

- **米国(USA):** GPSの近代化（Block III/IIIF衛星によるL1C信号等の提供）を継続し、PNT情報の一層の信頼性向上を目指している¹⁸²。2020年の大統領令13905号「測位、航法、タイミングサービスの責任ある利用を通じた国家レジリエンスの強化」に基づき、PNT国家R&D計画が策定され、GPSへの過度な依存を避け、多様な代替PNT技術の開発と重要インフラの防護を推進している⁴。連邦通信委員会(FCC)も、GPSを補完・代替するPNT技術の開発支援策を検討している⁴。
- **欧州連合(EU):** 独自のGNSSであるGalileoシステムにおいて、オープンサービス向けの航法メッセージ認証(OSNMA)を導入し、スプーフィング耐性を強化している²⁵。EU宇宙戦略では、PNTを含む宇宙アセットのセキュリティとレジリエンス強化、戦略的自律性の確保が重要課題とされている¹⁰²。欧州委員会は、GNSSと地上系サービスを組み合わせた強靭な「タイミングバックボーン」の構築も目指している²⁵。
- **ロシア(Russia):** GLONASSシステムを運用し、軍事利用においてはジャミングやスプーフィング技術を積極的に活用しているとされ、その影響はウクライナ紛争やバルト海地域などで広範囲に及んでいる⁴。一方で、2004年には米国との間でGPSとGLONASSの電波周波数適合性維持などに関する協力声明も発表されているが⁴、近年の地政学的状況下ではその実効性は疑問視される。
- **中国(China):** BeiDouシステムのグローバル展開を完了し、一带一路構想(BRI)やデジタルシルクロード(DSR)を通じて、その利用を国際的に推進している¹⁸⁵。BeiDouは地上局ネットワークと組み合わせることで高いPNT精度を提供し、中国のソフトパワー拡大に寄与している¹⁸⁵。一方で、中国沿岸での船舶スプーフィング事例など、国家による干渉への関与が疑われるケースも報告されている⁵²。

これらの主要宇宙大国は、自国のGNSS能力向上（多くは耐性強化機能を含む）を進めると同時に、一部の国は干渉能力の開発・展開にも関与していると見られている。この状況は、PNTが共有される地球規模の公益であると同時に、戦略的競争の舞台でもあるという複雑な地政学的力学を生み出している。各国が「PNT自律性」を追求する動き¹⁰²は、この二重性を象徴している。

国際機関の役割と提言(Roles and Recommendations of International Organizations)

GNSS干渉問題への対応において、国際機関は基準策定、情報共有、協力促進などの重要な役割を担っている。

- **国際電気通信連合 (ITU):** 無線周波数の国際的な分配、無線通信規則の策定・施行、干渉調整を担う国連の専門機関である¹。ITUは、無線航行衛星サービス(RNSS)用周波数帯の保護を加盟国に強く要請しており⁴⁸、世界無線通信会議(WRC)-23では、特定の周波数帯におけるGNSSおよびRNSSの有害な干渉からの保護を促す決議676が採択された⁴⁹。
- **国際民間航空機関 (ICAO):** 航空分野におけるGNSS利用に関する国際標準・勧告方式(SARPs)を策定し、干渉リスク評価や対策を勧告している²²。世界航空航法計画(GANP)への干渉対策の反映や、加盟国へのリアルタイム情報共有、アンチジャミング・アンチスプーフィング技術の開発・導入促進などを提言している⁷⁹。
- **国際海事機関 (IMO):** 海事分野におけるGNSS利用の安全基準(SOLAS条約等)を定め、干渉による航行安全への影響について警告を発している²²。加盟国に対し、RNSSの保護、従来型航法インフラの維持、関係当局間の協力強化、包括的な干渉報告メカニズムの実施などを求めている¹⁸⁶。
- **国連宇宙空間平和利用委員会(COPUOS) / 国際GNSS委員会(ICG):** ICGは、GNSS提供者と利用者の間の自発的な協力を促進するための非公式なフォーラムであり、GNSSシステム間の互換性・相互運用性の向上、干渉検知・軽減(IDM)技術に関する議論、情報共有、能力構築支援などを行っている¹。ICGのシステム・信号・サービス作業部会(WG-S)では、スペクトラム保護、LEO-PNTや月PNTとの互換性・相互運用性などが議論されている¹³⁰。また、IDMに関する3つの柱（プロバイダー、ハードウェア、エンドユーザー）に基づくレジリエンス強化策を提言している²⁰。

国際協力の現状と今後の展望 (Current Status and Future Prospects for International Cooperation in Spectrum Protection and Interference Mitigation)

周波数保護、干渉源の特定と情報共有、対策技術の標準化などにおいて、国際協力は一定の進展を見せている。ICGのようなフォーラムは、GNSS提供国間の技術的調整や情報交換に貢献している²⁰。しかし、これらの国際的な取り組みの実効性は、PNTの軍民両用性（デュアルユース）と、一部の国家主体が戦略的目的のために干渉行為を行う（あるいはその能力を保持する）現実によって制約を受けている。ITU決議においても、国家安全保障や防衛目的の干渉を例外とする場合があることが示唆されており¹⁹⁰、これはPNTの安定供給という地球益と、各国の安全保障上の利益との間に緊張関係が存在することを示している。このため、国際的な規制や協力の呼びかけだけでは、特に国家が関与する意図的な干渉を完全に抑制することは困難であり、真のレジリエンス確保は、外交努力に加え、技術的な堅牢性の追求と多様な代替手段の確保に大きく依存すると考えられる。

7. GNSS信号干渉の将来展望と克服すべき課題 (Future Outlook and Challenges to

Overcome in GNSS Signal Interference)

GNSS信号干渉の脅威は、技術の進歩とともに常に進化しており、将来的にもその巧妙化・高度化が予測される。これに対し、対策技術もまた進化を続けるが、克服すべき課題は依然として多い。

干渉技術の高度化・巧妙化と新たな脅威の出現 (Increasing Sophistication of Interference Techniques and Emergence of New Threats)

- **AI/MLを活用した適応型ジャミング・スプーフィング攻撃:** 将来的には、AIや機械学習（ML）を利用して、受信環境や対策技術をリアルタイムに学習・適応し、より効果的にGNSS利用を妨害するジャミング・スプーフィング攻撃が出現する可能性がある⁵⁷。これらは、従来の静的な干渉パターンとは異なり、予測や対策がより困難になることが予想される⁶⁶。
- **サイバー攻撃との融合:** GNSS受信機や関連システムへのサイバー攻撃と、電波干渉を組み合わせた複合的な脅威が増加する可能性がある⁸。例えば、受信機のソフトウェアの脆弱性を突いて誤動作させたり、認証情報を窃取したりした上で、スプーフィング攻撃を仕掛けるといったシナリオが考えられる。
- **宇宙空間からの干渉:** 衛星に搭載されたジャマーや、指向性エネルギー兵器など、宇宙空間から広範囲にGNSS信号を妨害する新たな脅威が出現するリスクも否定できない⁸。これは、特に広域インフラや国家安全保障に対する深刻な脅威となりうる。
- **干渉技術のアクセシビリティ向上:** ソフトウェア無線（SDR）技術の発展や、オープンソースの信号生成ツールの普及により、高度な干渉攻撃を実行するための技術的・経済的ハードルが低下している²⁶。これにより、国家以外の主体（テロリスト、犯罪組織、あるいは個人）による巧妙な干渉攻撃が増加し、脅威がより広範かつ予測困難になる可能性がある。

対策技術の進化、標準化、および社会実装の動向 (Evolution of Mitigation Technologies, Standardization, and Societal Implementation Trends)

脅威の進化に対応するため、対策技術も継続的に進化している。

- **AI/MLによるインテリジェントな干渉検知・対処:** AI/MLを活用し、干渉信号のパターンを学習・識別し、異常をリアルタイムに検知、さらには最適な軽減策を自動的に選択・実行するインテリジェントな受信システムの開発が進められている⁴⁵。
- **信号認証技術の普及:** GalileoのOSNMA、GPSのChimera、QZSSのQZNMAといった信号認証技術が実用化され、対応受信機への搭載が進むことで、スプーフィングに対する基本的な防御層が形成されることが期待される⁵⁵。
- **次世代PNT技術の実用化:** LEO-PNTコンステレーションの構築⁴や、量子センサー¹²¹、eLoran⁸⁴といった代替PNT技術の実用化が進み、GNSSへの依存を低減し、PNT情報源の多様化によるレジリエンス向上が期待される。
- **国際標準・認証制度の確立:** GNSS受信機や関連機器の耐干渉性能に関する国際的な標準規格や認証制度の整備が進むことで、一定レベル以上の対策が施された製品の普及が促進される¹⁴。

EUSPA（欧州連合宇宙プログラム庁）のレポートでは、マルチ周波数対応、高度なPNT処理戦略、アンテナ設計の進歩、そしてGalileo OSNMAのような認証機能、複数アンテナを持つ耐性型受信機、センサーハイブリッド化などが将来の重要なトレンドとして挙げられている¹⁰⁰。また、GNSS耐干渉ソリューション市場は、防衛や重要インフラのニーズを背景に大幅な成長が見込まれており、AI/ML統合やマルチコンステレーション対応が主要な技術トレンドとなっている¹⁴⁴。

宇宙空間からの干渉源探知・特定技術の可能性 (Potential of Space-based Interference Detection and Localization Technologies)

地上からのGNSS干渉源を、逆に宇宙空間から探知・特定する技術も研究されている。LEO衛星コンステレーションに搭載されたセンサー（GNSS-Rペイロードに類似したものなど）を利用して、地上や海上から放射される干渉波を検出し、その位置を特定する試みである⁴⁶。この技術が実用化されれば、広範囲を効率的に監視し、特にアクセスが困難な海域や他国領土内からの干渉源に対しても、ある程度の情報収集が可能になることが期待される。

GNSSの頑健性（レジリエンス）向上のための多層的アプローチの重要性 (Importance of a Multi-layered Approach to Enhance GNSS Resilience)

GNSS干渉の脅威は多様かつ進化し続けるため、単一の対策技術に依存するのではなく、複数の防御層を組み合わせた多層的なアプローチが不可欠である。これは、衛星系PNT（GNSS、LEO-PNT）、地上系PNT（eLoran等）、自律系PNT（INS、Visual SLAM等）といった異なる物理原理に基づくPNTソースを適材適所で組み合わせ、「システム・オブ・システムズ」として全体のPNTレジリエンスを確保するという考え方である⁴。Iridium STLのようなLEOベースの補完システムは、そのような多層防御の一翼を担う¹²⁸。さらに、ハードウェア（耐性型受信機・アンテナ）、ソフトウェ

ア（高度な信号処理アルゴリズム、AI/ML）、運用手順（干渉検知時の対応プロトコル）、そして政策・規制（周波数管理、不法電波の取り締まり）といった各レベルでの包括的な対策を講じることが、真のPNTレジリエンス確立には不可欠である²⁰。

社会経済的影響の評価と持続可能なGNSS利用環境の構築 (Assessment of Socio-economic Impacts and Establishment of a Sustainable GNSS Operational Environment)

GNSS障害が社会経済に与える影響は甚大である。英国政府の試算では、GNSSが長期間利用不能になった場合、1日あたり10億ポンド（約1900億円）の経済損失が生じるとされている⁹。米国においても、1ヶ月間のGPS停止で約582億ドル（約8.7兆円）、短期間でも1日あたり10億ドルの損失との試算がある¹¹。これらの試算は、GNSSが現代経済の基盤としていかに重要であるかを示している。

このような甚大な影響を回避するためには、重要インフラにおけるPNT依存度の正確な評価と、それに基づくリスク管理体制の強化が急務である³。GNSS脆弱性に対する認識の高まりは、単なる技術的対策を超え、PNTレジリエンスを国家戦略上の優先課題として位置づける動きへと繋がっている。これは、PNTがもはや単なるユーティリティではなく、能動的な保護と多様化を必要とする重要な国家資産として認識され始めたことを意味する。米国の大統領令13905号に基づく国家PNT R&D計画⁸²、国際機関による加盟国への行動喚起⁴⁸、耐干渉ソリューション市場の成長¹⁴⁴、そしてQZSSやGalileo OSNMAのような各国独自のPNT自律性・耐性強化の取り組み¹⁰²などは、このパラダイムシフトの現れと言えるだろう。

8. 結論と提言 (Conclusion and Recommendations)

GNSS信号干渉問題の重要性と継続的取り組みの必要性 (Reiteration of the Significance of GNSS Interference and the Need for Continuous Efforts)

本報告書で詳述してきたように、GNSSは現代社会の神経系とも言える不可欠な社会基盤であるが、その信号の脆弱性に起因する干渉問題は、偶発的なものから悪意のある攻撃まで多様化・深刻化しており、我々の生活や経済活動、安全保障に対する広範かつ重大なリスクとなっている。干渉技術と対策技術は「いたちごっこ」の様相を呈しており、脅威は常に進化し続けるため、この問題に対する継続的な警戒、研究開発、そして国際的な協調体制の強化が不可欠である。

技術開発、政策推進、国際連携強化に向けた具体的提言 (Specific Recommendations for Technological Development, Policy Advancement, and Strengthening International Cooperation)

GNSS信号干渉の脅威に効果的に対処し、PNTサービスの持続的な信頼性を確保するため、以下の提言を行う。

技術開発 (Technological Development):

1. 耐干渉型受信機・アンテナ技術の高度化と普及促進:
 - 適応フィルタリング、RAIM/ARAIM、CRPAなどの既存技術の性能向上、小型化、低コスト化を推進し、より広範なユーザーセグメント（民生機器を含む）への搭載を促進する。
 - 特に、スプーフィングに対する防御の要となる信号認証技術（OSNMA、Chimera、QZNMA等）の国際標準化を加速し、全ての新規GNSS受信機への搭載を奨励する。
2. AI/MLを活用した次世代型干渉検知・特定・対処技術の研究開発強化:
 - 未知の、あるいは適応的に変化する干渉パターンをリアルタイムに検知・分類し、最適な対処法を自律的に選択・実行可能なインテリジェントPNTシステムの開発を国家プロジェクトとして推進する。
 - 多様かつ大規模な実環境干渉データセットの構築と共有を進め、AIモデルの学習と検証を加速する。
3. 代替PNT技術の実用化加速と社会実装:
 - LEO-PNT、eLoran、量子センサー、慣性航法システム、Signals of Opportunityなど、GNSSとは異なる物理原理に基づく多様な代替PNT技術の研究開発を支援し、早期実用化と重要インフラへの段階的導入を促進する。
 - これらの代替技術とGNSSをシームレスに統合し、状況に応じて最適なPNTソースを自動選択するセンサー・フェュージョン技術の高度化を図る。

政策推進 (Policy Advancement):

1. 国内におけるGNSS干渉に関する法規制の整備・執行強化:
 - 電波法に基づき、意図的なGNSS信号妨害（ジャミング、スプーフィング）に対する罰則を明確化・厳格化するとともに¹⁴⁹、不法なジャマー等の製造・販売・所持・使用に対する取り締まりを強化する。
 - 偶発的干渉を未然に防ぐため、電子機器の電磁両立性（EMC）基準を強化し、市場監視を徹底する。

2. **重要インフラ事業者に対するPNTレジリエンス確保策の指針策定と導入支援:**
 - 電力、通信、金融、交通などの重要インフラ分野におけるPNT依存度評価を定期的に実施し、その結果に基づいた事業継続計画（BCP）の策定を事業者に求める。
 - 代替PNTシステムの導入や耐干渉型受信機の装備など、レジリエンス強化策の導入に対する技術的・財政的支援制度を検討する。
3. **QZSS「みちびき」の高度化とサービスの安定運用:**
 - 計画されている7機体制への早期移行と、将来的な11機体制への拡張を着実に進め、日本独自の持続測位能力を確立する⁸⁷。
 - 信号認証サービス（QZNMA）および公共専用信号の安定的な提供と利用拡大を図り、国内PNTインフラの信頼性を向上させる。
4. **干渉インシデント報告・情報共有体制の強化:**
 - 国内外で発生したGNSS干渉インシデントに関する情報を迅速に収集・分析し、関係省庁、重要インフラ事業者、研究機関、一般利用者の間で共有するためのプラットフォームを構築・運用する。

国際連携強化 (Strengthening International Cooperation):

1. **国際機関を通じたルール形成と周波数保護:**
 - ITU、ICAO、IMO、ICGなどの国際機関における議論に積極的に参画し、GNSS用周波数帯の国際的な保護、干渉許容基準の策定、意図的干渉の禁止といったルール形成を主導する。
2. **GNSS提供国・地域間での協力:**
 - 主要なGNSS提供国・地域（米国、EU、ロシア、中国、インド等）との間で、システムの互換性・相互運用性の向上、干渉情報や対策技術の共有、宇宙空間の安定的利用に関する対話を継続・強化する。
3. **国際共同研究・実証実験の推進:**
 - GNSS干渉の検知・特定・軽減技術や、代替PNT技術に関する国際共同研究プロジェクトや実証実験を積極的に推進し、知見と技術の国際的な共有を図る。
4. **宇宙空間の安定的利用に関する国際規範形成への貢献:**
 - 宇宙空間からの干渉といった新たな脅威に対し、宇宙空間の平和的かつ持続可能な利用を確保するための国際的な規範作りや信頼醸成措置に積極的に貢献する。

GNSS信号干渉問題は、技術、政策、国際協力が複雑に絡み合う地球規模の課題である。本報告書が提示した現状分析と将来展望、そして提言が、この課題に対する我が国の取り組みを一層深化させ、より安全で信頼性の高いPNT利用環境の実現に資することを期待する。

引用文献

1. GNSSの理解: 仕組み、主要システム、アプリケーションのすべて, 5月 29, 2025にアクセス、
<https://www.taoglas.com/jp/understanding-gnss-what-it-is-and-how-it-works/>
2. GNSS and Satellite Navigation Explained - Inertial Labs, 5月 29, 2025にアクセス、
<https://inertiallabs.com/gnss-and-satellite-navigation-explained/>
3. sites.calian.com, 5月 29, 2025にアクセス、
<https://sites.calian.com/app/uploads/sites/11/2025/01/Calian-AntiJamming-GNSS-Antenna-A250122WP-WEB.pdf>
4. docs.fcc.gov, 5月 29, 2025にアクセス、
<https://docs.fcc.gov/public/attachments/DOC-410031A1.pdf>
5. CRPA Antennas Explained: Choosing and Testing the Best Anti-Jam Solutions for GPS/GNSS Resilience - Spirent, 5月 29, 2025にアクセス、
<https://www.spirent.com/blogs/crpa-antennas-explained-choosing-and-testing-the-best-anti-jam-solutions-for-gps-gnss-resilience>
6. GNSS timing solutions - u-blox, 5月 29, 2025にアクセス、
<https://www.u-blox.com/en/time>
7. Quasi-Zenith Satellite System (QZSS) First Quasi-Zenith Satellite System 'MICHIBIKI' - Japan Aerospace Exploration Agency, 5月 29, 2025にアクセス、
https://global.jaxa.jp/countdown/f18/pdf/presskit_michibiki_e.pdf
8. Internet-exposed GNSS receivers pose threat globally in 2024 ..., 5月 29, 2025にアクセス、
<https://securelist.com/internet-exposed-gnss-receivers-in-2024/114548/>
9. The Problem with GNSS (Understanding Resilient PNT) | Insights ..., 5月 29, 2025にアクセス、
<https://steatite-embedded.co.uk/insights/tech-explained/the-problem-with-gnss-understanding-resilient-pnt/>
10. How GNSS Receivers Empower Smart Cities | Septentrio, 5月 29, 2025にアクセス、
<https://www.septentrio.com/en/learn-more/insights/how-gnss-receivers-empower-smart-cities>
11. Counting the cost of GPS vulnerability: Why the US needs a terrestrial backup - Blog - Adtran, 5月 29, 2025にアクセス、
<https://www.blog.adtran.com/en/counting-the-cost-of-gps-vulnerability-why-the-us-needs-a-terrestrial-backup>
12. Strengthening PNT to Avert Economic Setbacks - Geospatial World, 5月 29, 2025にアクセス、
<https://geospatialworld.net/prime/technology-and-innovation/strengthening-pnt-to-avert-economic-setbacks/>
13. GNSS干渉, 5月 29, 2025にアクセス、

