ChatGPT

GNSS信号干渉問題に関する調査報告

はじめに

GNSS（全球測位衛星システム）は現代の社会インフラや軍事活動に不可欠な位置・航法・時刻（PNT）情報を提供する。しかし、その微弱な衛星信号は**電波干渉**の脅威にさらされており、意図的・非意図的な妨害による悪影響が報告されている [1]。近年、航空・海上交通や通信へのGNSS干渉事案が世界的に増加し、国際民間航空機関（ICAO）や国際電気通信連合（ITU）、国際海事機関（IMO）など国際機関もその深刻な影響に対し「重大な懸念」を表明して加盟国へ対策強化を促している [1] [2]。本報告書では、GNSSに対する信号干渉問題について、これまでの主な歴史的経緯、代表的な干渉の種類、過去に発生した主要事例、各国（特にアメリカ、日本、ヨーロッパ）の対応策や法規制の動向を概説する。さらに将来の技術的・制度的課題と対策の見通し（耐干渉技術の開発動向、法整備の方向性、商業・軍事用途ごとの対策など）についても考察する。

GNSS信号干渉の概要と種類

GNSSは米国のGPSをはじめ、欧州のGalileo、ロシアのGLONASS、中国のBeiDou、日本の準天頂衛星システム（QZSS）など複数の衛星測位システムの総称であり、地球全域に測位・航法・時刻サービスを提供する。GNSS衛星から届く信号は非常に微弱（地上では数十ワット程度の電球を宇宙空間から見るほどの強度）であるため、他の電波による妨害を受けやすい。この**電波干渉**（RFI: Radio Frequency Interference）は大きく意図的なものと非意図的なものに分類できる。非意図的な干渉には、太陽フレアなどの自然現象や、他の無線機器による偶発的な周波数帯重複・機器故障などが含まれる [3]。一方、意図的な干渉には**ジャミング（妨害電波）**と**スプーフィング（なりすまし信号）**という代表的な手口が存在する。

- **ジャミング（Jamming）：** GNSS受信機が衛星信号を受信できなくなるよう、同じ周波数帯に強力なノイズや無意味な電波を送り込み受信環境を麻痺させる攻撃である [4] [5]。ジャミングが行われると受信機は正しい測位ができなくなり、位置や時刻情報の提供が停止する。ジャミング電波は安価な違法装置（「GPSジャマー」等）で容易に発信可能であり、近年ではインターネット上で作り方が拡散するなどして不正利用が増えている [6]。なお強力なジャミングは悪意なく誤って発生する場合もあり、例えば周辺周波数帯の送信機からの漏れ電波がGPS帯に混入する事例も報告されている [6]。

- **スプーフィング（Spoofing）：**GNSS衛星になりすました偽の信号を送り、受信機に誤った測位解を計算させる高度な攻撃手法である [7] [5]。スプーフィング攻撃では、本物の衛星信号と同じ形式だがわずかに遅延・変更を加えた電波を送信することで、受信機を誤作動させ意図しない位置・時刻を表示させる。これにより、GPSを用いるドローンや車両を意図したコースから逸脱させたり、船舶や航空機に誤った位置を信じ込ませることが可能になる。スプーフィングは高度な技術や装置を要し、従来は軍事目的で研究されてきたが、近年は個人でも安価なソフトウェア無線機などで実施できる可能性が指摘されている。スプーフィング攻撃が成功すると被害も深刻であり、対象の移動体のハイジャックや、位置情報に依存する地理的フェンス（立ち入り禁止区域管理）の突破、さらに交通・電力などインフラの制御システムへの影響など、多岐にわたるリスクを生じる [8]。

補足:　　これら以外にも、受信した真の衛星信号を記録・時間差再送信して欺瞞を行う**ミーコニング**（meaconing）と呼ばれる古典的手法も知られているが、広義にはスプーフィングの一種と見なされる。また、GNSSの利用者側での対策が困難な**衛星側からの妨害**（敵対的な衛星による妨害電波の発射など）も軍事的には想定されているが、現時点で具体的事例は多く報じられていない。

歴史的経緯と過去の主要事例

GNSS信号に対する妨害は、GPSが初めて運用された1990年代から軍事分野でその可能性が認識されていた。しかし本格的に社会問題として認識されたのは2000年代以降である。GPSが民生に解放され普及するにつれ、GNSSの脆弱性に着目した妨害行為や事故が顕在化した。以下に主な歴史的事例を挙げる。

- **2007年（米国サンディエゴ）：** アメリカ海軍の停泊中の艦船でGPS妨害装置が誤って作動し、市街地で大規模な電波障害が発生した [9]。この事故では空港の管制・ATMネットワークや病院システムにまで影響が及び、原因究明まで数日を要したと報告されている [10]。このケースは故意ではないジャミングでも社会インフラに深刻な支障をきたすことを示した。

- **2009〜2012年（韓国・北朝鮮）：** 北朝鮮は繰り返しGPSジャミング電波を発射し、韓国のソウル首都圏（仁川空港周辺）で民間航空機や船舶の運航に障害を起こした [11]。特に2012年には16日間連続で妨害電波を発信し続け、韓国で**1016便の航空機と254隻の船舶**に影響が及んだことが確認されている [11]。この挑発行為により着陸進入中の航空機が他空港へのダイバート（目的地変更）や着陸復行を強いられる事態となり、GPS依存の危うさが浮き彫りとなった。

- **2017年6月（黒海沿岸）：** ロシア周辺の黒海付近で、航行中の**20隻以上**の船舶がGPSスプーフィング被害に遭った [12]。各船舶のGPS受信機は実際とは異なる偽の位置座標を示し、航跡表示がおかしくなる現象が報告された。これは公に報じられた中では代表的な大規模スプーフィング事例であり、「サークル・スプーフィング」（複数船舶の表示位置が円形に集まる怪現象）として注目された [12]。

- **2017〜2019年（ロシア・北極圏）：** ロシア軍は2017年以降、欧州北部・北極圏の高緯度地域において断続的にGPS電波妨害を実施したとされる [13]。ノルウェーやフィンランドの当局によれば、2018年前後に両国の国境付近で民間航空機が度重なるGPS信号ロストを経験しており、その原因はロシア側からの強力なジャミングであったと報告されている [14]。欧州管制機関Eurocontrolは2018年以降、GNSS干渉報告件数が**2000%増加**したと指摘しており [14]、北極圏や東欧での紛争に関連した意図的干渉が一因と分析されている。

- **2019年7〜11月（中国・上海周辺）：** 中国の上海港やその周辺海域で、多数の船舶が同時期にGPSのスプーフィング被害を受けた [15]。**300隻以上**の船舶位置が誤った地点に偽装表示されるという大規模な現象が観測され、上記黒海事件と類似した「円を描くように船位がずれる」スプーフィングパターンが確認された [15]。専門家は、この現象は港湾に停泊する特定の船舶（例えば制裁逃れのタンカー等）を隠匿する目的で発生させられた可能性を指摘している。

- **2022〜2023年（ウクライナ紛争地域・東欧）：** ロシアによるウクライナ侵攻に伴い、戦域および周辺国でGNSS妨害が多発した。ウクライナ東部ではロシア軍がGPS妨害装置を展開し、ウクライナ軍や支援する西側諸国の無人機・ミサイル誘導を妨げようとする電子戦が繰り広げられたと報じられる [16]。その影響は周辺の民間領域にも及び、2023年初頭には北欧やバルト海周辺で民間航空機がGPS信号遮断や偽情報を受ける事例が相次いだ [17]。例えば2023年後半にはフィンランドやエストニアで旅客機が着陸直前にGPSを喪失し非常用の計器着陸に切り替える事態が発生している。国際的にも同年末から翌年初めにかけて東バルト海地域一帯で広域的なGPS妨害と「サークルスプーフィング」が確認され、民間航空の安全に影響が出たと報告された [17]。

以上のように、GNSS妨害は当初は軍事的な局所事例が中心であったが、2010年代以降は民生インフラへの影響事例が各地で表面化し、近年では紛争地帯周辺のみならず平時の都市圏でも発生している。また手口も高度化・大規模化する傾向にあり [18]、GNSSの安全利用を脅かす重大な課題となっている。

各国および国際機関の対応策と法規制の動向

GNSS信号干渉問題への対応は各国で法整備と技術開発の両面から進められている。特にアメリカ、日本、ヨーロッパの主要国・地域では、GNSSが社会基盤であるとの認識から早期に対策に乗り出してきた。また国際機関もガイドライン策定や各国調整を行っている。以下では主な国・地域・機関の取り組みを概説し、表1に各国の対応を比較する。

アメリカ合衆国の対応

アメリカではGPSを運用する立場上、早くからGNSS妨害対策を国家安全保障の重要課題として位置づけている。法律面では**連邦法によりあらゆる種類のジャミング装置の使用・販売・輸輸入が明確に禁止**されている[19]。連邦通信委員会（FCC）は「携帯電話ジャマーやGPS妨害器を用いて他者の通信を意図的に妨害する行為は違法であり、違反者には高額な罰金や機器没収、禁錮刑が科されうる」と警告している[20]。実際、2013年にはニュージャージー州でトラック運転手が違法GPSジャマーを使用していた事件でFCCが3万2千ドルの科料を科した例がある[21]。また法執行機関も2014年に高級車盗難グループがGPSジャマーで追跡を逃れていた事案に対しFBIが摘発を行うなど、犯罪への悪用対策も取られている[22]。

政策面では、アメリカ政府はGNSSへの依存リスク低減のための包括的戦略を策定している。2020年には大統領令13905号「PNTサービスの責任ある利用による国家レジリエンス強化」が発出され、連邦政府および重要インフラ事業者に対しGNSS妨害に備えたリスク管理とバックアップ確保を初めて包括的に指示した[23]。さらに2018年「国土安全保障法改正」において2020年までにGPSに代替可能なタイミング供給システムを用意するよう求める条項（Timing Resilience and Security Act）が成立し、陸上無線による時刻配信網の整備検討が進められた[24]。技術開発面では、軍用GPSの新しいMコード信号への更新（強力な送信出力と暗号化による抗干渉性向上）、軍用機やミサイル向けの耐ジャミングアンテナ（ビーム形成や周波数ホッピング技術）の配備が進められている。またGPS以外の補完PNT技術への投資も活発で、低軌道衛星を利用した新たな測位システムや、かつて廃止した長波無線航法Loranの復活強化版である**eLoran**の導入評価も行われている。例えばアメリカ沿岸警備隊は2020年にGPS受信妨害が海事に与える影響警告を発し、産業界に対し代替PNTの活用を促した[24]。現在、米国は衛星測位への依存を減らし「GPSが使えなくても安全に機能し続ける」レジリエントなインフラの構築を目指している。

日本の対応

日本においても、GPSを含む電波妨害行為は電波法により厳しく規制されている。**無線局の免許なく電波を発射することは一部例外を除き禁止**されており、違反した場合は1年以下の懲役または100万円以下の罰金が科せられる[25]。従ってGPSジャマーの所持・使用は違法であり、国内でも警察が妨害器の摘発や輸入規制の監視を行っている。

政府レベルでは、GNSS干渉対策も含めた衛星測位システムの強靭化が進められている。日本は米GPS補完目的で独自の準天頂衛星システム(QZSS，愛称「みちびき」)を整備しており、2020年代半ばまでに現行4機体制から7機体制（将来的には11機体制も検討）へと拡充する計画である。QZSSはGPSと互換性のある信号を提供して測位精度を高めるとともに、災害時等にGPSが使えない場合のバックアップ衛星として機能することが期待されている。

さらに日本は**信号認証サービス**という新たな対策を導入予定である。これはGNSSの航法メッセージに電子署名を付与し、その信号が正規の衛星から送信された本物であることを受信機側で検証できるようにする技術で、GNSSスプーフィング対策として注目される[26]。日本のQZSSによる信号認証サービスは2024年度から開始予定で、準天頂衛星の信号だけでなくGPSやGalileoの民生用オープンサービス信号についても認証情報を提供する計画である[27]。これにより、自動運転や航空・鉄道など安全性が重視される分野でもGNSSの位置・時刻情報をより信頼性高く利用できるようになると期待される[28]。加えて、日本は政府機関向けに暗号化された測位信号（QZSSの公共専用サービス）の提供準備も進めている。公共専用信号は欧州GalileoのPRS

や米GPSの軍用コードに相当するもので、防衛省や海上保安庁などが利用しうる。暗号化により一般に公開されていない秘匿性を持ち、ジャミングやスプーフィングに高い耐性を備えるとされる [29]。このように日本は法律による禁止と罰則、衛星システムの拡充、信号認証や暗号化技術の導入など多層的な対策を講じつつある。

ヨーロッパの対応

ヨーロッパではEU及び各加盟国が協調してGNSS妨害への対策に取り組んでいる。欧州連合の衛星測位システムGalileoは、構想段階からサービスの信頼性確保が重視されており、民生向けの**オープンサービス(OS)**に加えて政府向けの**公共規制サービス(PRS)**という抗干渉性の高いサービスを提供している [30]。**Galileo　PRS**は暗号化された信号で、認可された政府機関のみが受信できる。高出力・広帯域の電波を使用し、軍用GPSに匹敵する対ジャミング性能を持つほか、万一妨害や偽電波が発生した場合にも検知しやすい設計となっている [31] [32]。このため欧州各国の治安機関や緊急インフラでは、将来的にPRSを利用したより安全な測位・時刻同期が期待されている [30]。

一方、民間利用者に対しても欧州は**オープンサービス・ナビゲーションメッセージ認証(OSNMA)**と呼ばれる新機能を実装中である。OSNMAはGalileo衛星が提供する無料の信号に付加情報として認証コードを載せるもので、受信機がデータ改ざんを検知できる仕組みである。2022年より試験運用が開始され、2023〜2024年にかけて一般提供が始まる見通しとされる。これは日本の信号認証サービスと同様にスプーフィング対策として機能し、対応受信機を用いれば偽のGalileo信号を識別可能となる。

法規制の面では、EU域内では各国が電波法制によりジャマー機器の所持・流通を禁じている。例えばイギリスやフランスでは、GPS妨害装置の使用は違法であり発見された場合には厳しい罰則が科される。もっとも**世界的にはGPSジャミングを明示的に違法としていない国も多く存在する**のが実情である [6]。欧州当局者はそうした法の抜け穴を懸念しており、EU全体での統一的取り締まり強化も議論されている。また、欧州航空安全庁（EASA）は紛争地域周辺で急増するGNSS妨害に対応して安全情報通報（SIB2022-02）を発出し、航空各社に対し「GNSS途絶や異常発生を前提とした運用」を推奨している [33]。具体的には、パイロットは航法に支障が出た際に速やかに従来型の慣性航法や地上無線標識へ切り替える手順を訓練しておくこと、管制当局はGNSS妨害事例を監視・共有すること、航空機メーカーは妨害検知技術を向上させること等が求められている。欧州ではこの他、陸上移動体や港湾での妨害検出ネットワーク構築、重要インフラに対するリスク評価とバックアップ策（例えばeLoran復活の検討や高度な原子時計の利用）など、多方面で対策が講じられている [34]。

その他の国・国際機関の動き

上記以外にもGNSS干渉への対応を強化する国が増えている。例えば**韓国**は北朝鮮からの度重なるGPS妨害に対抗するため、世界に先駆けて長波無線航法Loran-Cを復活させた**eLoranシステム**の全国展開を進めている [35]。2010年代に北朝鮮の妨害で漁船が一斉に帰港する事態が発生したことを受け [35]、韓国政府は2016年に旧Loran局を改修して2020年までに3局体制のeLoran試験網を構築し、将来的にGPSに替わる陸上測位網として運用する計画である。韓国以外にも、ロシアや中国などGNSSを運用する国々はそれぞれ自国システムの暗号化信号（ロシアGLONASSの軍事コード、中国BeiDouの特権サービスなど）を保有し軍事利用時の干渉対抗策を講じているとみられる。またイスラエルなどGPSに依存する国では、国内で違法ジャマーを検出・摘発する監視網を設けるなどの措置も取られている。

国際機関では、先述のICAO・ITU・IMOの共同声明 [1] [2] のように、各国政府への注意喚起と協調行動の呼びかけが行われている。特にITUは電波主管庁として、各国に対しGNSSが属する**無線航法衛星業務（RNSS）**の周波数帯を他用途から保護する義務を再確認している [36]。また各国に対しては、「GNSSに頼るシステムのレジリエンス強化」「万一に備えた従来型航法インフラの維持」「通信・航空・海事・防衛・捜査当局の連携強化」「妨害発生時のITU等への通報」等を具体的に推奨している [37] [38]。ICAOも衛星航法の信頼性確保を航空安全上の最重要課題と位置づけ、各国航空当局に対し妨害発生時の代替経路設定やパイロット教育

を求めている。IMOも海事分野でのGNSS妨害増加に警鐘を鳴らし、電子海図システム(ECDIS)のみに依存しない伝統的航法の訓練継続や、港湾での干渉源探知能力向上を加盟国へ要請している。これら国際的な取り組みは、GNSSがもはや単一国の問題ではなく全世界共通の重要インフラであることを踏まえ、各国の協調した対策推進を目指すものである。

表1: 各国・地域におけるGNSS干渉への主な対応策の比較

国・地域	法規制の対応状況・措置	技術的な対策・主な取り組み例
アメリカ	- GNSS妨害装置の使用・販売を連邦法で全面禁止。違反者へ厳罰 [20] - 2018年法律でGPS代替のバックアップ時刻網整備を義務化 [24] - 2020年大統領令で重要インフラのPNTレジリエンス向上を指示 [23]	- 軍用GPS「Mコード」導入（暗号化・高出力で耐干渉性強化） - 耐ジャミングアンテナや受信機フィルタの開発・配備 - eLoran（長波航法）復活の実証実験、衛星以外のPNT技術研究 - 妨害検出ネットワーク（米沿岸警備隊による通報システムなど）
日本	- 電波法で無免許の電波発射（ジャマー使用）を禁止 [25] - 妨害波発信源の捜索体制（総務省・警察庁の無線監視システム） - 宇宙基本計画で衛星測位の信頼性向上を明記（2023年改定）	- 準天頂衛星システム(QZSS)の整備・衛星数増強（7機体制へ） - 信号認証サービス開始（2024〜、GPS・Galileo含め電子署名でスプーフィング検知） [27] - QZSS公共用暗号化信号の提供準備（抗干渉の政府専用サービス） [29] - マルチGNSS受信の推進（複数衛星系で冗長性確保）
ヨーロッパ (EU)	- 各国でジャマー違法化（英・仏などで厳罰化） - 欧州委員会がGNSS脅威に関する調査・法制提言を実施 - 欧州航空当局(EASA)が安全情報を通達（干渉時の運用指針） [33]	- Galileo衛星によるPRS（政府向け高信頼サービス）運用 [31] - Galileo OSNMA機能提供（民生向け信号認証でスプーフィング対策） - 欧州各国でeLoran再導入の検討（英仏で試験実施例あり） - 妨害検知・測位妨害源追跡の技術開発（欧州宇宙機関等の研究プロジェクト）
国際機関	- ITU: GNSS周波数保護の勧告、各国への妨害報告制度呼びかけ [36] - ICAO: GNSS障害時の航空安全対策ガイドライン策定 - IMO: 航海分野でのPNTバックアップ推奨（天測・無線航法の再評価）	- 各国連携の監視データ共有（例: ICAOの干渉データベース構築検討） - 衛星測位シグナルの認証標準化（ICGにおける各GNSSの相互運用検討） - 欧米主導での新技術評価（低軌道衛星による補完測位などの国際実証）

今後の技術的・制度的課題と対策の見通し

GNSS干渉問題に対処するため、今後さらに技術面・制度面双方での強化が求められる。商業利用分野と軍事利用分野でのニーズの違いも踏まえつつ、将来の課題と対策の方向性を以下にまとめる。

技術面における耐干渉技術の強化

技術的対策としては、まず**受信機側の耐干渉性能向上**が重要である。具体的には、高性能な**アンチジャミングアンテナ**（干渉源の方向に指向性Nullを作るなど）や、高帯域フィルタによる妨害信号の除去、複数周波数・複数システムの同時利用による冗長性確保が挙げられる。特にマルチGNSS受信により、一つの衛星系や周波数が妨害されても他から補完できる可能性が高まる。また、先進的な受信機では入力信号の**指紋検出（フィンガープリント）**によって偽信号を識別する研究も進む [39]。例えば受信信号の強度や到来方向の不自然さからスプーフィングを疑うアルゴリズムや、衛星ごとの電波特性差異を検出して本物かどうか判断する

技術である。加えて、前述の**ナビゲーションメッセージ認証**（データにデジタル署名を付与）は今後標準的な防御策となる見込みだ。欧州GalileoのOSNMAや日本の信号認証サービスに加え、米GPSも将来の世代では民生信号への認証導入（チップレベルでのメッセージ認証: CHIMERA計画等）が検討されている [39] 。

さらなる新技術として、衛星測位に依存しない**オルタナティブPNT**の活用が展望される。例えば地上長波によるeLoranは衛星とは周波数帯も原理も異なるため、GNSSとは共通の脆弱性を持たない独立系として有望視される [40] 。実際、韓国やイギリスでは限定的ながらeLoran送信網が運用・試験されている。他にも、高高度擾乱に強い**慣性航法装置(INS)**との統合、電波以外の**視程航法（地磁気や重力異常、星球測位の活用）**の研究など、多角的な代替手段が模索されている。近年では民間企業が打ち上げた大量の低軌道通信衛星（例: SpaceX社のStarlink網）の通信信号を流用して測位や時計同期を行う試みも報告され、従来のGNSSに頼らない新たなPNTインフラの可能性が広がっている。

制度面における課題と法整備の方向性

制度・政策面では、まず**違法ジャミング機器の流通抑止と摘発強化**が引き続き課題である。インターネット通販を通じた小型ジャマーの入手は今も容易であり、各国の電波当局や税関における取締体制の国際連携が必要となる。また、現行法では電波利用の国内違反に対する罰則はあっても、**国家ぐるみで行われる越境的なGNSS妨害への制裁**は明確でない。例えばある国が隣国領域に向けて妨害電波を発射しても、現実には国際法で直ちに処罰する仕組みは無い。今後、ITUや国連を通じてこのような**意図的干渉行為を軍事紛争下の電子戦行為と区別し民生被害を減らす枠組み**を検討する必要があるとの声もある。さらに各国国内に目を転じると、GNSSに依存するクリティカルインフラ（通信・交通・金融など）事業者に対し**PNTサービス中断への備え（レジリエンス計画）を義務付ける規制**も今後進むと予想される。米国では既に大統領令や法令で重要インフラ事業者に対しリスク評価と対策を求めており、日本や欧州でも同様のガイドライン策定が検討されている。例えばイギリス政府報告書では、もし5日間に渡り全国でGNSSが使用不能となった場合、経済損失は推定52億ポンド（約7800億円）に上るとの分析もあり [41] 、各国政府はPNTの確保を国家安寧に関わる問題と捉え始めている。

商業用途・軍事用途における対策の展望

GNSS干渉への対策は、**商業用途**（民間利用）と**軍事用途**でアプローチが異なる面もある。商業分野ではコストやオープン性の制約から、公的サービスによる広域対策や業界標準の枠組み作りが鍵となる。例えば航空・海運業界では国際標準に沿った干渉検知装置の搭載やパイロット教育が進み、携帯通信や電力業界では自社ネットワーク内でGNSS時刻に異常が生じた際に自動で警報・切替を行う仕組みを整備しつつある。またGNSSメーカー各社も、高精度受信機にアンチスプーフィング機能やジャミング検出ログ出力機能を付加する製品を開発している [34] 。今後は異業種間での情報共有（例えば港湾で妨害発生時に空港へ通知）や、公共部門と民間部門の協力（妨害発生源の追跡に通信事業者の協力を得る等）が一層重要になるだろう。

軍事用途では、従来から**電波妨害下での作戦遂行能力**が重視されてきた。各国軍隊は暗号化された抗干渉性の高い測位信号（米GPSのMコード、欧州GalileoのPRS、ロシアや中国の軍用コードなど）を運用し、また受信機側でも電子戦対抗仕様のアンテナやフィルタを採用している。さらにGPSに頼らない自己完結型の航法として高性能INSや地図マッチング技術を組み合わせ、一定時間GNSSが使えなくとも精密誘導を継続できるよう工夫している。また、敵によるGNSS妨害自体を探知・無力化する電子戦能力（妨害発信源の位置特定と破壊など）も軍の重要任務となっている。一方で軍事においてもGNSSは完全ではなく、近年の紛争ではGPSが妨害された状態でドローンやミサイルを運用するケースが相次いだ。これを受け、米軍やNATOは**「GPSなしでも戦える」戦術の再訓練**や、複数の測位手段を併用するシステム構築を急いでいる。

おわりに

GNSSに対する信号干渉の問題は、その歴史が示す通り年々深刻化しつつある。ジャミングやスプーフィングは一国の安全保障だけでなく、航空機や船舶の航行、安全運行システム、金融取引の時刻認証など幅広い民

生領域にも影響を及ぼしている。各国は法規制の整備と技術開発によって対策を講じてきたが、妨害手段も巧妙化・拡散化しており**「いたちごっこ」の様相**も呈している。今後、衛星測位の安全な利用を維持するためには、技術面では多層防御とバックアップ手段の確保、制度面では国際協調による厳格な取り締まりとインフラ事業者へのレジリエンス義務化など抜本策が求められる。幸いにも国際社会はGNSSの重要性を共有し始めており [42]、ICAOやITUのように各国横断的な取り組みも動き出した [36]。GNSSは「見えざる公共財」とも呼ぶべき存在であり、その安定運用を守ることはデジタル社会と安全保障の基盤を支えることである。技術進歩と適切な制度整備によって、将来にわたり安心してGNSSを利用できる環境を構築していくことが期待される。

---

[1] [2] [5] [36] [37] [38] [42] Press Release
https://www.itu.int/en/mediacentre/Pages/PR-2025-03-25-radio-navigation-satellite-service-harmful-interference.aspx

[3] [4] [6] [7] GPS jamming: the benign, the bad, and the scary | Flightradar24 Blog
https://www.flightradar24.com/blog/inside-flightradar24/types-of-gps-jamming/

[8] [14] [22] [24] [34] [39] [41] Momentum Builds to Fend Off GNSS Jamming, Spoofing - EE Times Europe
https://www.eetimes.eu/momentum-builds-to-fend-off-gnss-jamming-spoofing/

[9] [10] [11] [12] [13] [15] [16] [17] [18] [26] [27] [28] [29] www8.cao.go.jp
https://www8.cao.go.jp/space/comittee/27-anpo/anpo-dai60/siryou2.pdf

[19] [20] [21] GPS.gov: Information About GPS Jamming
https://www.gps.gov/spectrum/jamming/

[23] Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services | US Department of Transportation
https://www.transportation.gov/pnt/executive-order-strengthening-national-resilience-through-responsible-use-positioning

[25] GPSジャマーをためしてみた
https://io.cyberdefense.jp/entry/gps%E3%82%B8%E3%83%A3%E3%83%9E%E3%83%BC%E3%82%92%E3%81%9F%E3%82%81%E3%81%97%E3%81%A6%E3%81%BF%E3%81%9

[30] [31] [32] Galileo Public Regulated Service (PRS) - Navipedia
https://gssc.esa.int/navipedia/index.php/Galileo_Public_Regulated_Service_(PRS)

[33] Global Navigation Satellite System (GNSS) Outages and Alterations | EASA
https://www.easa.europa.eu/en/domains/air-operations/global-navigation-satellite-system-outages-and-alterations

[35] South Korea Developing an eLoran Network to Protect Ships from Cyber Attacks - Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and Design
https://insidegnss.com/south-korea-developing-an-eloran-network-to-protect-ships-from-cyber-attacks/

[40] South Korea discusses decision to combine GPS and eLoran
https://geospatialworld.net/blogs/south-korea-discusses-decision-to-combine-gps-and-eloran/