2025 年度

卒　業　論　文

ジャミング・スプーフィングの調査及び スプーフィングのドップラ RAIM による検知

学科名　流通情報工学科

学籍番号　2223015

氏名　岡田悠聖

指導教員　久保信明

目次

第1章　序論

1.1 研究背景

衛星測位システムは米国が 1978 年に GPS(Global Positioning System)衛星を打ち上げ、1995 年に正式にサービスが開始されて以降、軍事から民間まで幅広く利用されるようになり、現在では誰もが利用できる身近なシステムとなった。米国の GPS に続き、現在はロシアの GLONASS(グロナス)、EU の Galileo(ガリレオ)、中国の BDS(北斗)、インドが Navic(ナビック)を開発しサービスを提供している。日本も GPS を補完・補強する目的の RNSS(Regional Navigation Satellite System/地域測位衛星システム)として QZSS(Quasi-Zenith Satellite System/準天頂衛星)を 2010 年から整備し、現在は 5 機の衛星でアジア、オセアニア地域をカバーしている。これらの衛星測位システムの総称として GNSS(Global Navigation Satellite System/全地球測位システム)が現在用いられている。

GNSS は自動車、船舶、航空機といった移動体の運航支援や情報通信の時刻同期、地震の検知等の防災目的など様々な場面・分野で活用がなされている。24 時間 365 日、安定して提供される位置、速度、時刻を情報源として多くのシステムが我々の生活を支えており、GNSS は社会インフラの一つとして機能していると言える。

一方で GNSS が持つ脆弱性を利用した妨害や不正も発生している。GNSS の電波妨害手法は主にジャミング(妨害)とスプーフィング(なりすまし)の 2 種類が存在する。ジャミングは GNSS 受信機が衛星からの信号を捕捉できないようにすることで測位不能にする。スプーフィングは GNSS 受信機を騙して、偽の位置や時刻を出力させる方法である。前者は工事現場や施工での妨害や空港システムの妨害が考えられる。後者に関しては UAV(無人航空機)などの自動運転、自動地着陸において、間違った方向へ勝手に飛んでいくといった危険がある。スプーフィングはジャミングと異なりシステム側で GNSS の情報が間違っていることを検知できなければ、偽の位置情報をもとにシステムが作動してしまうため、単純に位置情報が取得できなくなるジャミングよりも脅威度が高いと考えられている。また、これらの妨害技術は年々低コスト化しており、GNSS に依存した社会において大きな脅威となっている。

GNSS を社会基盤として利用していくうえで、このような脅威から守るための措置や対処方法の確立は急務であり、課題解決に社会的意義がある。以上を背景として本論文ではジャミング・スプーフィングによる影響や防御手法に関する研究内容について論じる。

1.2　研究の目的とアプローチ

本論文では特に危険度の高いスプーフィング攻撃が第三者から行われたとき、これを検知する手法を提案することを目的とする。研究の目的を達成するために以下のアプローチで GNSS スプーフィングの研究を行った。

(1) ジャミング・スプーフィングによる事故事例と近年の対策研究

まず実社会におけるジャミング・スプーフィングの影響や事故事例を把握する。また、今日に至るまでどのような防御・対策手法の研究が行われているのかを調査し、それぞれの特徴や有効性をまとめた。そこから得られた情報によって、想定されるスプーフィングの種類とそれによる被害を推察し、求められているスプーフィング対策の方向性を明らかにすることを目的とした。

(2) GNSS の妨害実験

GNSS の妨害に際して実際に使用される、ジャマー、スプーファーと呼ばれる装置の仕組みや性能を理解することを目的として、出力を確認する実験と実際にスプーフィングをする実験を行った。

(3) 観測ドップラと予測ドップラによるスプーフィング検知

スプーフィング信号と衛星からの正しい信号が混在している場合、ドップラ測位による PVT(Position, Velocity, Timing)解が歪むため、観測ドップラと PVT から生成した予測ドップラの差分に変化が現れる現象を利用したスプーフィングの検知手法を提案した。本手法では GNSS 受信機のスプーフィングを行うために GNSS SDR(Software Defined Radio/ソフトウェア受信機)を用いて実験を行い、提案手法の有効性や弱点を評価した。

1.3 論文の構成

まず、第 2 章において GNSS の脆弱性とスプーフィングをはじめとする妨害手法の理解や本研究に用いた理論の理解に必要な GNSS 測位技術の概要を説明する。

第 3 章では実社会で発生したジャミング・スプーフィングの影響や事故事例や近年の防衛・対策手法を調査する。

第 4 章ではジャマー・スプーファーを用いて GNSS の妨害実験を行うことで、それらの機器の性能評価や市販受信機の評価を行う。

第 5 章では提案手法である観測ドップラと予測ドップラによるスプーフィング検知について述べる。検知アルゴリズムと実験結果、考察を示す。

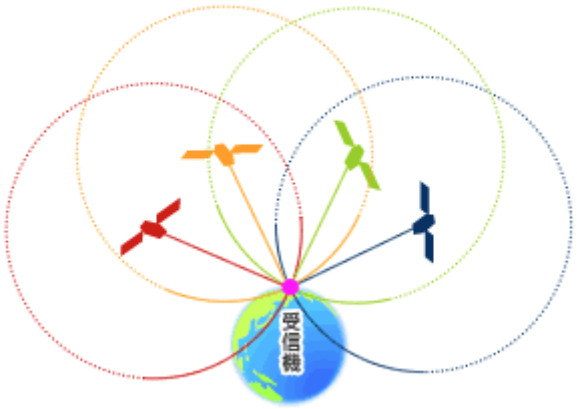
第 6 章では本研究の総括と今後の課題や展開について示す。

第2章　GNSS の概要

本章では現在の GNSS 測位の概要、各国による GNSS の運用状況、GNSS における測位手法の違いについて述べる。

2.1　GNSS 測位の概要

GNSS は 4 つ以上の衛星を用いて、各衛星とユーザーの受信アンテナ間の距離を測距用のデジタル信号を用いて測ることで、ユーザーの地球上の絶対位置を計算するシステムである。GNSS 衛星は地球をあらかじめ決められた軌道で周回し、決められたタイミングとパターンに従って測距用信号を放送している。距離は電波の伝搬時間から計算するが、正確な距離を測るためには衛星と受信機の時計が正確に同期している必要がある。しかし、受信機の内部時計と衛星に搭載されている原子時計には誤差 t が存在するため、ＧＮＳＳ測位では 3 次元座標の x,y,z と時刻誤差 t の 4 つの未知数を求めるために、最低 4 本の距離の線が必要となる。したがって GNSS 測位では最低 4 機以上の衛星から同時に信号を受信する必要がある。4 機以上の衛星から測位電波を同時に受信し、4 元連立方程式を解くことで自身の位置と時刻を同時に得ることができる。4 機以上の衛星から電波を受信して測位するイメージ図を図 2-1-1 として示す。



(出典) https://www.jaxa.jp/countdown/f18/overview/gps_j.html

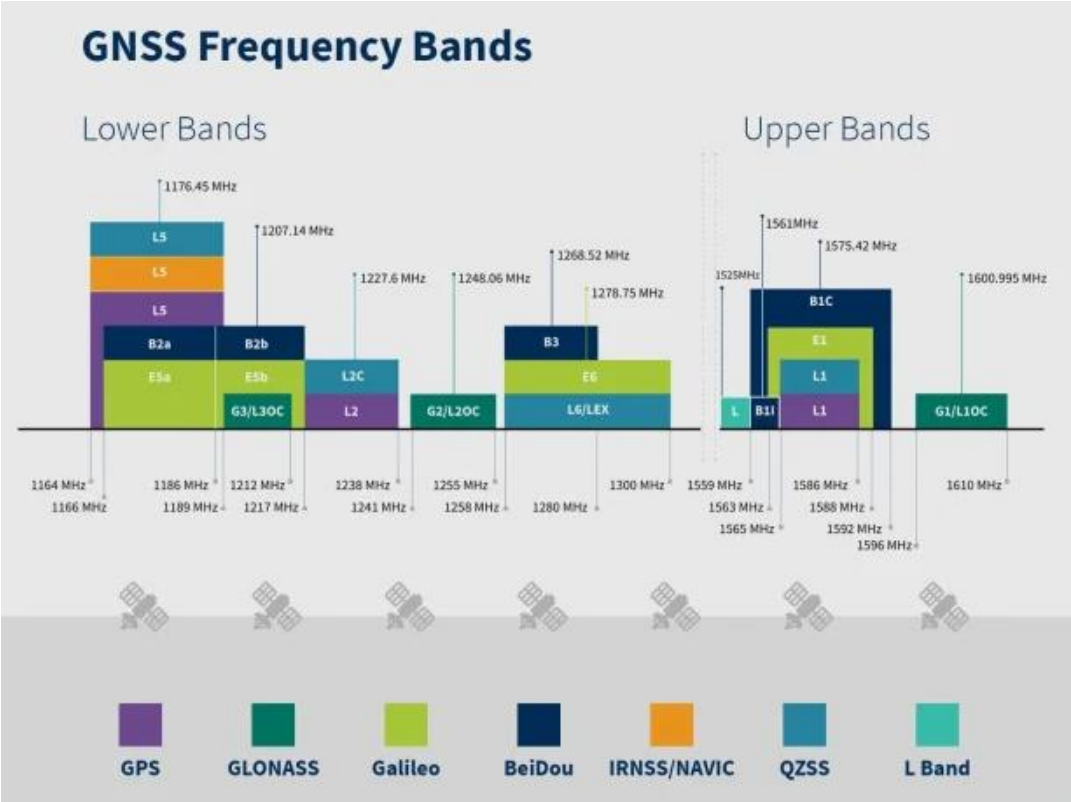
図 2-1-1　GNSS 測位のイメージ図

衛星は高速で軌道上を動いているためドップラ効果によって、受信した電波は本来の中心周波数から若干のシフトが生じる。これを用いると衛星・ユーザー間の相対速度を計算することが可能で、さらに衛星の速度は提供される軌道情報(エフェメリス)から既知であるため、相対速度ベクトルから衛星の移動速度ベクトルを引くことで最終的に地球に対するユーザーの絶対速度ベクトルを計算することができる。

GNSS を用いて得られるこれらの情報は PVT(Position, Velocity, Timing)と呼ばれる。

また地上の GNSS 受信機では衛星からの信号を受信する際に、送られてきた航法メッセージを復調解読している。これは衛星から送られる測距用信号は複数の中心周波数が存在する。GPS

を例に挙げると、L1(1575.42MHz)、L2(1227.60MHz)、L5(1176.45MHz)という 3 つの L バンド搬送波に測距情報を載せて放送している。衛星ごとに使用されている周波数帯は次の図 2-1-2 で紹介する。



(出典) https://www.taoglas.com/blogs/navigating-l1-l2-and-l5-band-options-for-gnss/

図 2-1-2　GNSS における衛星の信号周波数帯

また、衛星からの信号は CDMA(Code Division Multiple Access)や FDMA(Frequency Division Multiple Access)、TDMA(Time Division Multiple Access)といった通信方式で放送される。

2.2　GNSS の脆弱性と妨害手法

GNSS 衛星から地表に到達する電力は非常に微弱であるためそれよりも大きな妨害信号をノイズとして受信機に与えてやれば、衛星からの信号はノイズに埋もれて正確に復調することが困難になる。GNSS のシステムは妨害に弱く、測位に影響を受けやすいという性質があり、対策が必要とされている。以下では主要な正規信号による測位を妨害する手法について述べる。

2.2.1　ジャミング

ジャミング(jamming)とは正規の電波通信と同一の周波数または周波数帯の電波を送出し、混信もしくは電波障害を引き起こすことにより、正規の通信を妨害することを指す。GNSS 以外では TV 放送、携帯ネットワーク、Wi-Fi、軍用無線などの無線通信に対して実施されることがある。GNSS であれば、2MHz ほどの帯域幅で妨害対象信号の中心周波数で雑音信号を発射する。

強い雑音が GNSS アンテナを通過し受信機で受信されることで、各衛星信号の SNR(Signal to Noise Ratio/信号雑音比)が低下する。SNR が低下していくと GNSS の測位精度が悪化し、最終的には信号追尾ができなくなり測位不能となる。GNSS では雑音に強い CDMA といった拡散方式が使用されており、復調時にジャミング波が拡散されて信号強度が低下するため、信号捕捉の妨害には 27dB 以上、信号追尾の妨害には 47dB 以上の J/S(Jamming to Signal Ratio/ジャミング信号比)が必要である。GNSS の空間中の信号強度は－130dBm ほどなので J/S が 27dB のときはジャミング波のアンテナ進入時信号強度は－103dBm 以上という GNSS の信号の 500 倍ほどのパワーを必要とする。ジャミングは送信する電波の帯域幅と尖頭出力にトレードオフの関係がある。そのため一般的に使用される狭帯域ジャミングは安価である代わりに 1 つの GNSS 信号帯域しかジャミングができない。一方、高価格で機器のサイズも大きいジャマーは狭帯域ジャミングと同じ出力で複数の GNSS 信号帯域を妨害することができる。

2.2.2　再放射

GNSS アンテナで受信した正規信号を増幅して、別のアンテナから再放射する方法も妨害の一つになる。リアルタイムの正規な信号を受けて、増幅して利用するこのような仕組みはリピーターと呼ばれ、屋内で GNSS の評価実験を行う目的に利用されることがある。欺瞞する位置はその時の欺瞞信号生成用の GNSS アンテナ位置となってしまうが、本物の GNSS 信号を使用するためリアルタイム性や欺瞞信号の信用度が非常に高い。一方でターゲットに攻撃者の位置がばれてしまうことが欠点として挙げられる。

2.2.3　ミーコニング

ミーコニング(Meaconing)とは本物の GNSS 信号を記録し、それを再放送する手法である。再放送と似ているが、再放射がリアルタイムな信号を放射するのに対して、ミーコニングは遅延や一部の改ざんを施して妨害を行う点で異なる。あらかじめ記録しておいた移動体の位置情報を、信号再生装置から送信してターゲットに誤った位置に誘導することが可能である。しかし、現実のリアルタイム時刻との同期は難しいため、時刻を監視しておくことでミーコニングを検出できる可能性がある。

2.2.4　スプーフィング

スプーフィング(Spoofing/なりすまし)とは偽の GNSS 信号を生成し、それを送信することでターゲット受信機に偽の PVT を測位させる手法である。GNSS 信号の生成コンピューターなどで行い、生成されたデジタルデータを RF フロントエンドと呼ばれるハードウェアでアナログ電波に変換して放射用のアンテナから出力する。この生成された欺瞞信号をスプーフィング信号と呼ぶ。

スプーファーはオープンサービス GNSS 信号の RF キャリア、PRN/拡散コード、データビッ

トを複製する必要がある。典型的な受信 GNSS 信号は以下の形式で表される。

$$y(t) = Re\left\{\sum_{i=1}^{N} A_i\, D_i\,[t-\tau_i\,(t)]C_i\,[t-\tau_i(t)]e^{j(\omega_c t-\phi_i(t))}\right\} \tag{2.1}$$

ここでは次のように文字が定義されるものとする。
N：拡散コードごとの構成信号の数、A_i：第 i 信号の搬送波振幅、
D_i(t)：データビット列、C_i(t)：拡散コード、$\tau_i(t)$：コード位相、
ω_c：公称搬送波周波数、$\phi_i(t)$：ビート搬送波位相、$v(t)$:受信雑音

スプーファーが送る偽信号の集合は同様に以下の式で与えることができる。

$$y(t) = Re\left\{\sum_{i=1}^{N} A_{si}\widehat{D}_i[t-\tau_{si}(t)]C_i[t-\tau_{si}(t)]e^{j(\omega_c t-\phi_{si}(t))}\right\} \tag{2.2}$$

Ns=N で、各信号は対応する真信号と同じ拡散コードを持ち、しばしば同じデータ列の最良推定$\widehat{D}_i$を放送する。
偽装された振幅、コード位相、搬送波位相はそれぞれ$A_{si}, \tau_{si}(t), \phi_{si}(t)\ (i = 1, \dots, N)$
これらの量は後述するように、実行される攻撃の種類によって変化するため、真の量と異なる可能性がある。

スプーフィング攻撃の間、被害者の受信アンテナでの全信号は

$$y_{tot} = y(t) + y_s(t) + v(t) \tag{2.3}$$

となる。ここで$v(t)$は受信ノイズである。場合によっては、このノイズがすべて自然に発生する。また、スプーファーが偽の信号に加えてノイズ成分を加えている場合もある。

再放射やミーコニングは正規の衛星からの信号を扱うのに対して、スプーフィングは偽の信号を作り出す点が異なる。任意の時刻や位置をシミュレートする信号を作り出すため、位置や時刻の欺瞞を自由にリアルタイムで設定することができる。スプーフィングデバイス GNSS 受信機を搭載し、それの時刻を使用することで本物の GNSS 信号と同期した時刻で欺瞞信号を生成することも可能であり、多様な攻撃目的に対応することができる。

スプーファーもジャマーと同様に安価なものと高価なものが存在する。安価なスプーファーは時刻同期性能や送信する GNSS 信号帯域に制限がある代わりに、入手が容易で簡単に妨害工作を行うことができる。一方で高価なスプーファーは時刻同期や、複数の信号帯域の欺瞞を行うことができるため、スプーフィングの検出は非常に困難になる。

第3章　GNSS 妨害による事故事例と近年の対策研究

GNSS は社会基盤として機能しており、多くの人が生活、業務かかわらず利用している。最近では RTK(Real Time Kinematic)や PPP(Precise Point Positioning)といった cm 級の高精度な測位手法がスマート農業や ICT、建築といった分野にも利用されており、将来的には移動体などの無人化にも応用される可能性が高い。しかし、GNSS の脆弱性によってどのような事故や犯罪が発生しているか理解している人は少ない。第 2 章で述べたように、GNSS の妨害手法は多岐にわたり利用場面も地上、海上、航空というように攻撃対象によって変化する。特にスプーフィングは目的ごとに欺瞞のシナリオを変化させるため、いくつかの検出手法が適用できない場合がある。そこで実際にスプーフィングによる事故事例を調査することによって、想定されるスプーフィングの種類とそれによる被害を推察する。同時に近年のスプーフィングによる妨害対策や防衛手法について調べることで求められている有効な検出手法やスプーフィングの特徴をつかむ。

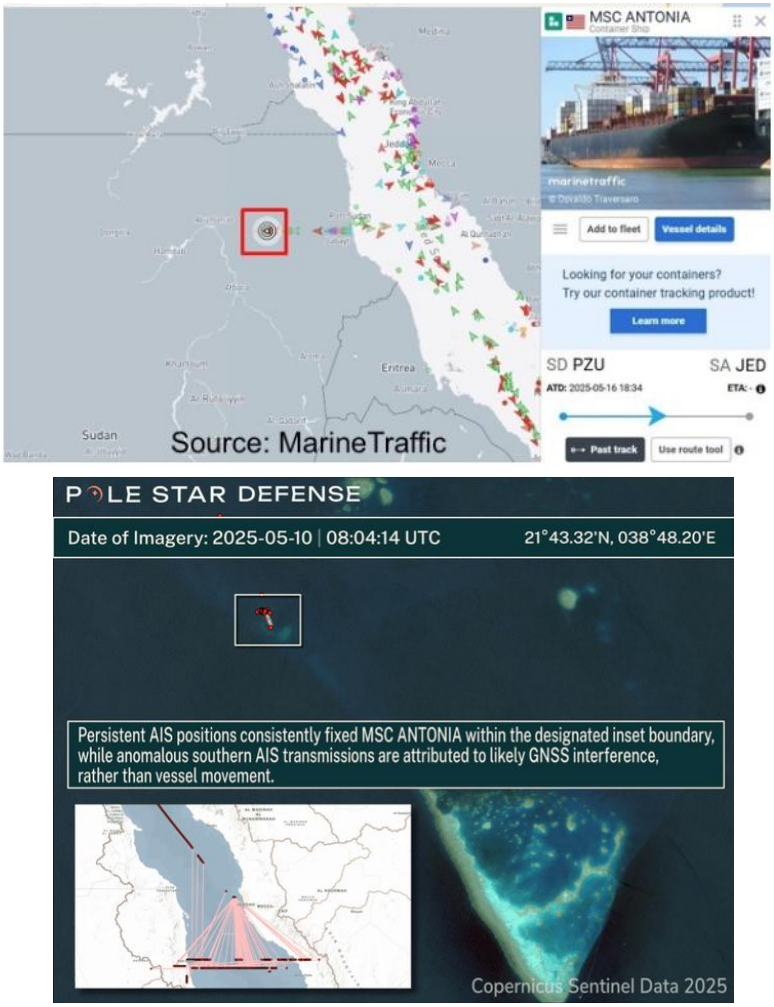
3.1　ジャミング・スプーフィングによる事故事例

船舶と航空機についてジャミングやスプーフィングがどのように使用され、事故発生に至ったかを記述する。また、事故以外にも代表的な GNSS 妨害が本学科の主要な研究テーマである物流にどのような影響を与えるのかについても記述する。

3.1.1 紅海におけるコンテナ船　MSC Antonia の座礁

2025 年 5 月 10 日、地中海・紅海航路で運航されていたコンテナ船 MSC *Antonia* が、サウジアラビア・ジェッダ港南西の紅海に位置する浅瀬帯 Eliza Shoals 付近で座礁する事故が発生した。MSC *Antonia* はリベリア船籍の約 7,000TEU 級コンテナ船であり、地中海と紅海を結ぶ定期サービスに投入されていた大型商船である。本船はスーダンの Marsa Bashayer からジェッダ港へ向けて航行中に予定針路から外れ、浅瀬に乗り上げたと報告されている。事故による負傷者は報告されておらず、また大規模な油濁等の環境被害も確認されていないものの、数日間にわたり座礁状態が続き、複数のタグボートによる離礁作業が行われた。

事故後に公開された AIS（Automatic Identification System）の航跡データによれば、MSC *Antonia* の位置情報は座礁前後において不自然な跳躍を繰り返しており、実際には浅瀬上に停止しているはずの船舶が、データ上では紅海の遠方海域や内陸部に瞬間的に出現するなど、物理的にあり得ない軌跡が観測された海事データ分析企業 Windward や複数の船舶トラッキングサービスは、このような AIS 上の挙動が、偽の GNSS 信号によって位置情報が改ざんされた際に典型的に見られる「スプーフィングパターン」と整合的であると指摘している。図 3.1 は事故当時の船の位置や航路情報を表したものです。



(出典) https://splash247.com/grounded-msc-ship-appears-in-the-sahara/

図 3.1　MSC Antonia の位置情報

さらに、海事インテリジェンス企業 Pole Star Global は、衛星画像と AIS データを組み合わせた解析結果を公表し、MSC *Antonia* の座礁は GNSS への意図的な干渉が主要因であった可能性が高いと結論づけている。同社の報告によれば、光学衛星画像上では本船が Eliza Shoals 上で静止している一方で、船上のナビゲーションシステムは偽の GNSS 信号に基づく誤った位置を受信していたとされる。このような状況下では、ECDIS（電子海図表示装置）と GNSS に強く依存したブリッジチームが、自船の実際の位置と危険浅瀬との相対関係を適切に把握できず、結果として座礁を回避できなかった可能性が指摘されている。

3.1.2　Azerbaijan Airlines Flight 8243 の墜落事故

12 月 25 日、ロシア着陸予定だったアゼルバイジャン航空機がカザフスタンに不時着し、38 名が死亡した。墜落の経緯は依然不明だが、現時点で入手可能な限られた証拠からは、同機がチェチェンへの着陸を試みた際にロシア防空システムが発射したミサイルによる損傷を受けた可能性が示唆されている。図 3.2 は事故後の航空機の写真である。

（出典）https://www.reuters.com/world/asia-pacific/kazakh-report-says-plane-dec-25-crash-probably-damaged-by-external-objects-2025-02-04/

図 3.2　墜落後の Azerbaijan Airlines Flight 8243

この事故は、ロシアによるウクライナ侵攻に伴い、南ロシア一帯で防空システムおよび電子戦システムの運用が常態化していた状況下で発生した。欧州航空安全機関（EASA）は、ロシア西部空域ではウクライナからのミサイル・無人機攻撃に対応する防空システムの作動により、民間機が誤って標的となるリスクが高まっていること、さらに紛争周辺では GNSS（GPS を含む）ジャミングおよびスプーフィングが継続的に発生していることを指摘している。その上で、EASA は 2025 年 1 月発行の紛争空域情報ブリテン（CZIB 2025-01）において、本事故をそうした高リスク空域における代表的な事例として挙げている。米連邦航空局（FAA）が 2025 年 12 月に公表した「GNSS 干渉リソースガイド」では、8243 便の飛行経過が次のように整理されている。同便はバクーからグロズヌイに向けて飛行中に GNSS ジャミングを受け、さらにスプーフィングとみられる現象が発生した結果、衛星航法を利用できなくなった。乗員は悪天候下で地上無線標識（NDB）を用いた計器進入を複数回試みたものの着陸に至らず、最終的に目的地からの離脱と代替空港へのダイバートを決定したとされる。GNSS ジャミング／スプーフィングとの関係については、航空安全情報会社や各種の技術解説が、ADS-B を用いた公開飛行データ解析等に基づき、8243 便が南ロシア上空で GPS 信号の喪失や位置情報の異常を繰り返し経験していたことを指摘している。ロイター通信が引用した専門機関の分析でも、同便は南西ロシア上空の飛行中を通じて GPS ジャミングの影響下にあったとされる。FAA の GNSS 干渉ガイドは、ジャミングおよびスプーフィングによって衛星航法が使用不能となったことが、困難な地上無線標識進入やダイバート決定を含む運航判断を複雑化させ、結果的に防空システムが作動する紛争周辺空域への長時間滞空を招いたと整理しており、本事故を「GNSS 干渉が運航リスクを顕在化させた典型例」として位置づけている。

3.2　物流におけるジャミング・スプーフィングの危険性

物流分野における GNSS は、車両や貨物の現在位置、移動履歴、到着予定時刻を把握するための基盤技術として不可欠な存在となっている。たとえば、トラックやトレーラーには GNSS 受信機を搭載した車載端末が広く導入されており、それらが取得した位置情報は携帯電話網等を介して配車システムや輸配送管理システムへ送信される。この情報に基づき、配車担当者は車両の稼働状況をリアルタイムに監視し、遅延が見込まれる場合には代替ルートの案内や別車両の手配といった対応を行うことが可能となる。また、コンテナやパレットに取り付けられたトラッカーを用いることで、海上輸送・鉄道輸送・トラック輸送を跨いだインターモーダル輸送においても貨物単位でのトレーサビリティを確保できる。さらに、近年普及が進む自動運転トラックや高度運転支援システム、港湾や倉庫内で運用される自律走行型搬送ロボットやドローン配送においても、GNSS は広域的な位置基準として利用されており、地図情報や各種センサと組み合わせることで、物流オペレーション全体の効率化や可視化に重要な役割を果たしている。

しかしながら、このような GNSS への依存度の高まりは、GNSS 信号に対する攻撃、とりわけジャミングとスプーフィングが物流システムにもたらしうる影響を大きくしている。ジャミングは、強いノイズ信号を送信することにより正規の衛星信号をかき消す攻撃であり、その結果として受信機は位置情報を取得できない、あるいは取得できても精度が著しく劣化する。物流の観点から見ると、長距離輸送車両の現在位置が突然取得不能になることで、運行管理側からは車両が「行方不明」となり、盗難やハイジャックなど異常事態の早期検知が困難になる。また、自動運転や隊列走行など GNSS を前提とした制御を行っている場合には、位置情報の喪失が制御アルゴリズムに負荷を与え、不自然な減速や車線維持の乱れを生じさせ、追突や車線逸脱といった事故のリスクを増大させる。港湾や空港周辺でジャミングが発生すれば、船舶や車両の入出場時の安全マージンが低下し、接触事故やオペレーション停止に至る可能性も否定できない。これに対してスプーフィングは、受信機に対して「もっともらしいが偽物の GNSS 信号」を送信し、誤った位置や時刻を信じ込ませる攻撃であるため、単なる測位不能状態よりも発見が難しく、物流に対してより深刻な影響を及ぼしうる。今後想定される被害として、まず貨物盗難への悪用が挙げられる。攻撃者が輸送中のトラック近傍で偽の GNSS 信号を送信し、車載端末に「正規ルート上の位置」を誤認させれば、運行管理システム上は車両が予定どおり走行しているように見える一方で、実際の車両は人気のない場所や不正積み替え地点へ誘導される。この結果、貨物が盗難に遭っても、管理側はしばらくの間異常に気づかず、被害の拡大や犯人特定の遅れを招く恐れがある。

次に、タクシー配車サービスにおける不正利用も想定される。タクシーやライドシェアにおいては、車両位置の把握や運賃計算、乗務員の勤怠管理などに GNSS が広く用いられている。スプーフィングにより車両位置が意図的にずらされると、実際には短距離しか走行していないにもかかわらず長距離運行を装ったり、逆に長距離走行を短く見せて不正な割引や裏取引を行ったりすることが可能となる。また、アプリ上の車両位置が改ざんされることで、本来配車すべき乗客から離れた車両に優先的に配車を回す、いわば「囲い込み」のような不正も理論上は成立しうる。このような不正は運賃の公正性やサービス品質を損ない、プラットフォーム全体への信頼低

下を引き起こす。

さらに、誤った配送が発生するリスクも見逃せない。宅配やラストワンマイル配送では、GNSS に基づいてルート最適化や配送先付近でのナビゲーションが行われている。スプーフィングにより配送車両や配達員の位置がずらされると、システム上は正しい住所に到達したと判定されてしまい、実際には類似住所や近隣の建物に誤配する可能性が高まる。これが多数の配送に対して同時に発生した場合、誤配や再配達が多発し、顧客満足度の低下だけでなく、人手と時間の大幅なロス、配送コストの増加といった経営的な悪影響も生じる。また、医薬品や重要部品など、特に厳密なトレーサビリティが求められる貨物において誤配送が発生すれば、安全性や信頼性の観点から重大な問題となる。

加えて、速度違反の隠蔽にもスプーフィングは利用されうる。多くの物流事業者は、安全運転管理の一環として車両の速度や走行履歴を GNSS ベースのドライブレコーダや運行記録装置で記録しているが、スプーフィングにより位置と時刻が改ざんされると、実際には高速道路等で制限速度を大幅に超えて走行していたとしても、記録上は「制限速度内での走行」として保存される可能性が生じる。個々の運転者が故意に自身の速度違反を隠蔽することも、組織的に過密な運行スケジュールを維持するために速度超過を黙認しつつ記録だけを改ざんする、といった不正も理論上は可能である。このような状況は、形式上は安全運転が守られているかのように見せかけながら、実態としては重大事故のリスクを高めるものであり、交通安全政策やコンプライアンスの観点からも大きな問題となる。

以上のように、ジャミングは主として GNSS 機能を一時的に麻痺させることで物流オペレーションの混乱や安全余裕の低下をもたらし、スプーフィングはもっと深刻に、貨物盗難やタクシー配車サービスでの不正、配送ミスの誘発、速度違反の隠蔽といった形で、物流システムの公正性および信頼性を根本から損ないうる。今後、物流分野で GNSS の利用がいっそう拡大することを踏まえると、GNSS 信号に対する攻撃を前提にしたフェイルセーフ設計や、多源センサによる冗長な位置推定、異常な位置・速度履歴を検出する仕組みを導入することが、物流の安全・安心を確保する上で不可欠になると考えられる。

3.3　近年のジャミング・スプーフィング研究

この節では近年のスプーフィング対策手法として提案されている航法メッセージ認証、補正インフラまで含めた防御、アレーアンテナ、SDR による信号監視、INS 支援トラッキングによる抑制の 5 つを調査、比較する。

各対策を「保護対象」「適用レイヤ」「成立条件」「残余リスク」の 4 点で比較する。ここで重要なのは、各手法が同じ検出器ではなく、守る対象が異なることである。例えば航法メッセージ認証は航法データの真正性を扱い、アレーアンテナによる DOA 推定は到来方向という物理層の証拠を扱い、INSAT は追尾ループの挙動を制御して誤差の増大を抑える。したがって、単純な優劣ではなく「用途・制約に応じた組合せ可能性」を比較の結論として導く。

（1）衛星サービス側の航法メッセージ認証：OSNMA

OSNMA は、Galileo が Open Service の航法データに認証情報（デジタル署名）を付与し、受信機が Galileo 由来であることを検証できるようにする枠組みである。OSNMA は 2025 年 7 月

24 日に運用宣言されたとされ、サービス定義文書（SDD）の公開とともに正式化されている。

この手法の最大の強みは、「衛星が送った航法データが本物かどうか」を暗号学的に検証できる点にある。従来の受信機側検知（相関波形の歪み、C/N0 変化、運動モデルとの不一致など）は、統計的・経験的な判断になりやすく、環境（マルチパス、遮蔽、受信品質低下）によって誤検知・見逃しが増え得る。これに対して NMA は、航法メッセージの起源と完全性を検証可能にし、少なくとも「偽の航法メッセージを新規に作って受信機を欺く」タイプの攻撃に対して、受信機が明確な根拠をもって排除・警告できる。さらに、衛星側で提供されるため、個々の利用者が高度な検知アルゴリズムや追加センサを用意しなくても、対応受信機であれば広域・一様に恩恵を受けられるという意味で、対策を仕組みとして普及させやすい利点もある。

一方で弱点もはっきりしている。第一に、NMA が直接保証するのは主として航法メッセージの真正性であり、受信を不能にするジャミングには効かない。また、攻撃者が正規の信号・メッセージを録音して遅延再送するようなリプレイ／メーコニング系の攻撃では、メッセージ自体は真正でも測距や時刻が攪乱され得るため、NMA だけで万全とは言えない（他の物理層・センサ融合・整合性監視が必要になる）。第二に、方式によっては鍵の遅延開示などの仕組みを使うため、認証が事後的になり得る（認証が確定するまでの遅延が生じる）という運用上の制約がある。第三に、利用するには受信機側の対応（ファーム更新、鍵・時刻同期、処理・電力コストの増加など）が前提で、普及途上では「対応端末と非対応端末が混在する」期間が長くなりやすい。総じて、NMA は強い根拠を与える基盤対策である一方、攻撃の全範囲を単独で覆うものではないため、受信機側の検知（DOA 推定、RTK 整合性、INS 支援追尾など）や運用監視と組み合わせた多層防御として設計するのが現実的である。

（2）補正インフラまで含めた防御：GNSS Corrections

GNSS Corrections（GNSS 補正情報）とは、GPS/Galileo/BeiDou/GLONASS などの測位に含まれる誤差を外部から補正し、位置精度・安定性（場合によっては信頼性）を向上させるための追加データの総称である。単独測位（単独受信機のみ）では、衛星軌道・衛星時計誤差、電離圏・対流圏遅延、受信機のハードウェア遅延、マルチパスなどの影響により、通常はメートル級の誤差が残る。補正は、これらの誤差要因を推定して利用者に配信し、受信機が観測値に適用することで、精度をセンチメートル級まで高めることを目的とする。

GNSS 補正を用いたスプーフィング対策の強みは、攻撃面を「受信機への RF スプーフィング」だけに限定せず、補正システム全体（基準局・配信路・クラウド処理）まで含めて防御設計できる点にある。高精度測位では、利用者端末は補正データに強く依存するため、仮に攻撃者が受信機だけでなく基準局や配信路、クラウド処理へ介入できれば、誤った補正が多数の利用者へ同時に波及し得る。この観点から、補正サービス側で衛星データや基準局観測を相互検証して外れ値を排除したり、異常局を隔離したり、補正ストリームの暗号化・完全性検証で配信改ざんを防いだりすることは、端末単体では困難な「広域波及リスク」を下げる有効なアプローチとなる。また、補正ネットワークが持つ多数局・多数データの冗長性を利用して整合性を確認できるため、受信機単独の統計的検知よりも、運用上は堅牢な監視・管理の枠組みを構築しやすい。

一方で弱点は、補正を用いる対策が本質的に補正サービスを信頼基点とする点にある。補正の

生成・配信・認証を担う事業者側が侵害された場合、逆にそれが単一障害点となって影響が広がる可能性がある。また、補正利用には通信や配信インフラが前提となるため、通信断や遅延、あるいはジャミングで GNSS 受信自体が不安定な状況では可用性が低下し、対策として成立しにくい場合がある。さらに、補正は「測位精度を上げる仕組み」であり、スプーフィングの形態によっては、補正データが常に決定打になるとは限らない。例えば受信機が完全に偽信号へ引き込まれて観測自体が汚染されている場合、補正側で整合性を担保しても、端末側の状態推定・追尾が破綻すれば効果が限定され得る。加えて、紹介記事のように産業界の設計思想として提示される内容は、学術論文のような統一条件下の定量比較が十分に示されないことも多くい。総じて、GNSS 補正を用いた対策は、受信機単体の検知を補完してシステム全体を守る方向に強みを持つ一方、信頼・通信・可用性といった運用前提に依存するため、受信機側の検知・抑圧や他の認証手段と組み合わせた多層防御として位置づけるのが適切である。

（3）アレーアンテナによる DOA 推定

アレーアンテナとは同じ種類のアンテナを規則正しく複数本並べることで、各々の素子の振幅および位相を独立に制御できるようにしたものである。アレーアンテナの写真を図 3.3 に示す。

図 3.3　アレーアンテナ写真

このアレーアンテナと MUSIC 法（Multiple Signal Classification）を用いた到来方向（DOA: Direction of Arrival）推定によるスプーフィング検知は、GNSS 信号が「衛星ごとに空の異なる方向から到来する」という幾何学的性質を利用する手法である。正規の GNSS 信号は、衛星の配置に応じて受信機へ多方向から入射する。一方、典型的なスプーフィングでは、攻撃者（スプーファー）が地上の単一送信機から複数 PRN の偽信号をまとめて放射するため、受信機から見ると「複数衛星に対応するはずの信号が、実際には共通の方向から到来する」という不自然さが生じる。本手法はこの差を検出根拠とし、複数素子のアレーアンテナで得られる受信信号の位相差から到来方向を推定し、複数 PRN で共通 DOA が観測される場合にスプーフィングを疑うという考え方である。

ただし GNSS では同時に多数の衛星信号が存在するため、MUSIC 法が要求する「到来信号数

がアンテナ素子数より少ない」という条件を満たしにくい。大阪公立大学らの研究では、GNSS の PRN コードを用いた逆拡散を前処理として用い、対象とする衛星信号成分を取り出して他成分を抑圧したうえで空間相関行列を作り、MUSIC スペクトルから DOA を推定する枠組みを採用している。これにより、GNSS の多信号環境でも MUSIC を適用可能とし、スプーフィング環境下の実験により検知可能性を示したとしている。

この手法の強みは、検知根拠が C/N0 や相関歪みといった受信品質指標ではなく、到来方向という「空間的特徴」にある点である。航法メッセージの改ざんや上位層のデータ操作とは独立で、物理層の制約に基づくため、攻撃者が整合を取るには、複数方向から衛星配置に見合った信号を再現する必要があり、攻撃コストを上げられる。また、DOA 推定は「検知」だけでなく、推定した妨害源方向に対してビームフォーミングやヌル形成を適用して偽信号を抑圧する、といった将来的拡張（検知→抑圧）にもつながる。さらに、複数 PRN で共通方向が出るという判定ロジックは直観的で説明しやすく、運用上のアラート根拠としても扱いやすい。

一方で弱点は、導入要件と攻撃モデルへの依存にある。第一に、アレーアンテナ（複数素子）とその較正が必要で、単一アンテナの一般的受信機や小型端末への適用は容易ではない。第二に、共通 DOA を根拠とするため、攻撃者が複数送信機を分散配置する、あるいはリレー等で見かけの到来方向を散らすといった分散型の攻撃には弱くなり得る。第三に、実環境ではマルチパスにより到来方向推定が乱れ、正規信号側にも見かけ上の共通方向が現れる可能性があるため、検知閾値や安定化処理が重要になる。加えて、逆拡散＋MUSIC の処理は計算量が増えやすく、リアルタイム運用ではハードウェア資源や処理遅延の評価が必要となる。

（4）SDR による信号監視

SDR による信号監視（マルチパスモニタリング）は、「スプーファーが単一送信源から複数 PRN の偽信号を放射する」という状況では、直接波と反射波（マルチパス）の関係が衛星間で似通うという点を利用した検知手法である。正規衛星信号でも直接波・反射波は存在するが、マルチパス遅延や信号強度の関係は衛星ごとに多様になりやすい一方、スプーフィング信号ではそれらが衛星間で一様になると予想されるため、本研究では直接波と反射波を同時受信して監視することでスプーフィング検知を行っている。

この SDR 監視方式の強みは、(1) 受信機の追尾過程で得られる相関・マルチパス指標を直接使うため、測位解が大きく破綻する前段で検知できる可能性があり、研究としても「素早い応答速度やコンパクト性」を狙っている点、(2) 特徴量が複数衛星で一様化するという空間的・物理的性質に依拠するため、単一指標の閾値判定よりも説明可能性を持たせやすい点にある。また SDR を用いることで、2ch（RHCP/LHCP）を同期させた解析や、LHCP 成分の追尾・相関値といった市販受信機では取得しにくい内部量にアクセスでき、検知ロジックを構成しやすい。

一方の弱点は、(1) 二偏波アンテナ＋2ch フロントエンド＋SDR という機材要件があり、一般受信機へそのまま移植しにくい点、(2) DBSCAN の eps 等のパラメータにより「検知感度を上げると平常時の誤検出が増える」というトレードオフが生じ、環境依存の調整が必要な点、(3) ハードウェア仕様の制約から、当面は GPS/Galileo/QZSS の 1 周波構成で最適化されている点である。

（5）INS 支援トラッキングによる抑制

INSAT（INS-Aided Tracking）は、スプーフィングを「検知して GNSS 観測を捨てる」方式（INS 単独運用に近い）ではなく、**受信機の追尾ループ（DLL/PLL）そのものを INS で支援して、偽信号ではなく真正信号へロックし続けることを狙う抑圧（mitigation）手法である。従来方式は長時間攻撃で INS 誤差が累積しやすい一方、INSAT は追尾ループが高電力信号を追いやすい性質を踏まえ、ループパラメータを適応的に調整して真正信号へ誘導し、誤差累積を根本的に避けることを目的としている。

この手法は追尾ループの判別器出力（I/Q のコヒーレント積分から得る誤差）を観測量、INS の状態を状態方程式として、ロバスト・カルマンフィルタで統合している。スプーフィングにより判別器誤差（残差）が増えると、残差に基づく適応係数（anti-spoofing factor）が低下し、観測ノイズ共分散を膨張させて判別器観測の重みを下げ、相対的に INS 状態を強く信頼する。これにより、コード位相・周波数や搬送波周波数を INS から推定して追尾ループを駆動し、たとえ偽信号が強くても真正信号へのロックを維持しやすくする。さらに偽信号と真正信号が分離して状況が回復すると、係数が戻って観測の重みが回復し、追尾ループが累積した INS 誤差の補正に再び寄与する。

一方で弱点（成立条件）も明確である。牽引中は加速度計・ジャイロのバイアス補正を停止するため、INS のバイアス不安定性が大きい場合や遅い牽引では INS 誤差が閾値を超えて真正信号から完全に乖離し、ロック喪失に至り得ると述べている。また偽信号の電力優位が極端に大きい場合、RF フロントエンドの AGC 動作で真正信号の C/N0 が低下し、優位 70 dB では C/N0 が 20 dB-Hz 未満となって追尾が成立せず、挙動がジャミングに近くなるという限界も示されている。

第4章　GNSS の妨害実験

この章では販売されているジャマーやスプーファーを使用して、その出力や効果を確認する。実験は第 4 実験棟 5 階の電波暗室にて行った。

4.1　ジャマーによる実験

海外で販売されているジャマーを使用し、その出力を確認する。使用した機器や実験手順について説明する。

4.1.1　実験対象と使用機器

本研究では，市販の携帯型 GPS 妨害装置を実験対象として用いた。対象装置は，ProJammer（Sigint Technology, Slovak-EU）が「GPS Anti-tracking jammers」として販売している EU-121G 型であり，GNSS の複数バンドに対して妨害信号を放射することを想定したポケットサイズのジャマーである。図 4.1 は使用したジャマーの写真である。

図 4.1　実験で使用するジャマー

EU-121G は上面に複数本のアンテナを備えた携帯型筐体を採用しており，L1〜L5 に相当する複数の GPS 周波数帯を同時にカバーするよう設計されている。公称ジャミング半径は最大 5–15 m 程度であり，周囲の電波環境や携帯電話事業者のネットワーク条件に依存するとされている。電源は AC100–240 V から 12 V への変換アダプタと，容量 1800 mAh の内蔵バッテリを併用する構成であり，バッテリのみで約 1 時間の連続動作が可能とされている。筐体寸法は 113 mm × 60 mm × 31 mm，質量は約 0.28 kg（本体のみ，カタログ値）であり，手のひらサイズで容易に携行できる。

4.1.2　実験方法

本節では，GPS ジャマー EU-121G の送信スペクトルおよび出力レベルを評価するために行った測定方法について述べる。実験は，外部への不要な電波漏洩を防ぐため，大学の電波暗室内において実施した。ジャマーからの出力は空間放射ではなく有線接続によりスペクトルアナライザに注入し，電波法上の問題が生じないよう配慮した。

(1) 機器構成

ジャマーの送信アンテナ端子を同軸ケーブルによってスペクトルアナライザの RF 入力端子に接続した。

(2) 測定条件および手順

スペクトルアナライザの中心周波数およびスパンは，EU-121G の公称送信周波数帯（GPS L1～L5 各帯域）を十分に含むよう設定した。分解能帯域幅（RBW）およびビデオ帯域幅（VBW）は，必要な周波数分解能を確保しつつノイズフロアが安定して観測できる値に設定し，測定ごとに同一条件を用いた。検波方式は平均電力の把握を目的として RMS 検波とし，必要に応じて最大値の確認のためピークホールド表示も併用した。本装置のアンテナ接続ポートには，筐体左端から順に ポート 1，2，3，4 の番号を付与した。

測定手順は以下の通りである。

1. 電波暗室内にジャマーおよびスペクトルアナライザを設置し，接地および電源配線を確認する。
2. スペクトルアナライザの周波数レンジおよび RBW/VBW 等の測定条件を設定し，ノイズフロアおよび基準レベルを確認する。
3. ジャマーの電源を投入し，対象とする周波数帯（L1，L2，…）を有効にした状態でスペクトルを観測する。必要に応じてトレース平均化を行い，安定したスペクトルを取得する。
4. 得られたスペクトルについて，主ローブの最大レベル，帯域幅，スプリアス成分の有無などを読み取り，記録する。
5. 測定対象のアンテナポートを変更し，残りのポートについても同様の手順で測定を繰り返す。

以上の手順により，送信ポートごとにジャマーの出力スペクトルを取得し，ジャマー送信端子における実効出力レベルを推定した。これらの結果を基に，後章において GNSS 受信機に対する妨害強度および影響範囲の評価を行う。

4.1.3　実験結果

それぞれのポートについて，L1 帯および 1.2～1.6 GHz の広帯域スペクトルを測定した結果を以下に示す。

図 4.2 にポート 1 の L1 帯における送信スペクトルを示す。周波数掃引範囲は 1.53～1.63 GHz，RBW は 10 kHz とした。図より，L1 帯のジャミング信号は 1566 MHz～1582 MHz の約 16 MHz 幅にわたる広帯域の雑音状スペクトルとして観測された。スペクトルアナライザ入力端でのピーク電力はおよそ −71 dBm であり，GNSS の空間中の信号強度-130dBm が十分埋もれる信号強度で妨害波を発生させていることが分かる。

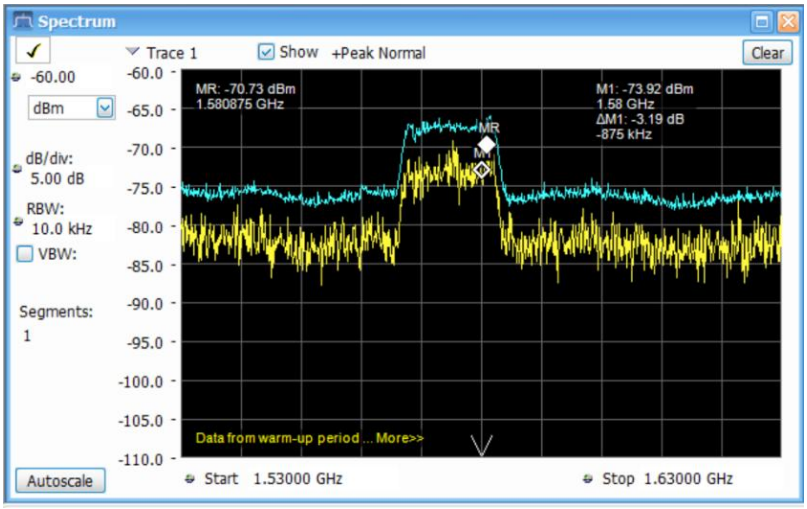


図 4.2　ジャマー：ポート 1 の送信スペクトル

同様の条件でポート 2，ポート 3 についても L1 帯のスペクトルを測定した。その結果を図 4.3 と図 4.4 で示す。

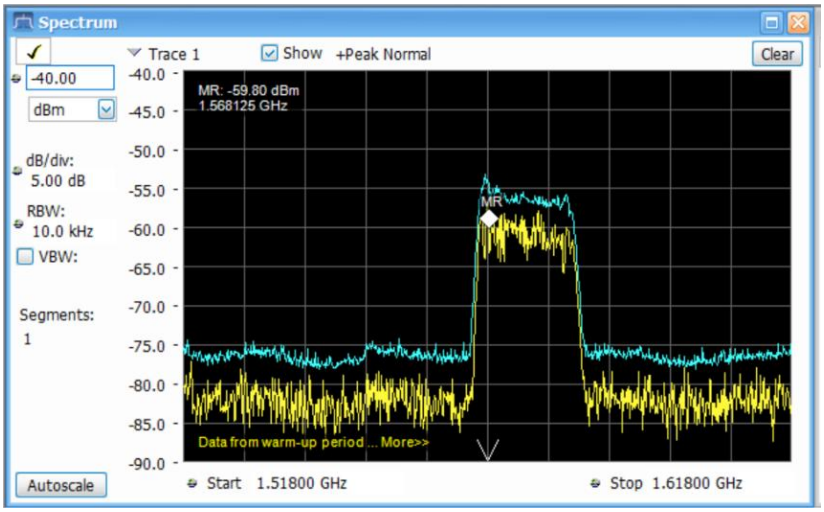


図 4.3　ジャマー：ポート 2 の送信スペクトル

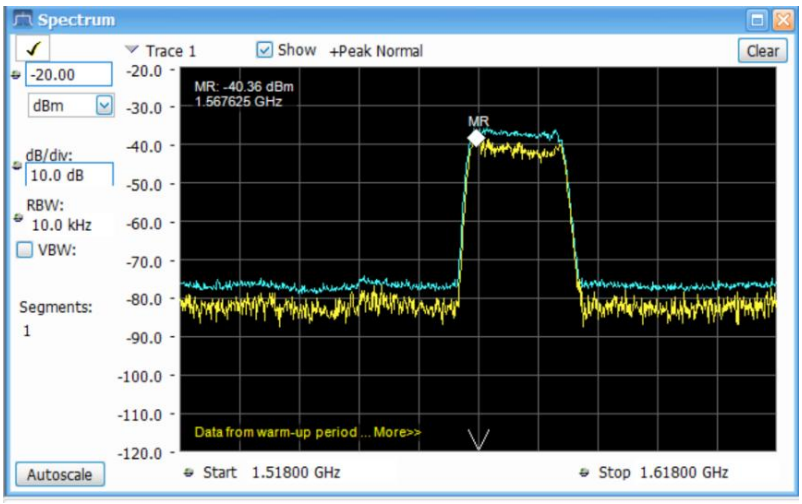


図 4.4　ジャマー：ポート 3 の送信スペクトル

ポート 2 とポート 3 はピーク電力がそれぞれ 約 −63 dBm，約 −40 dBm となった。いずれのポートにおいても，主なジャミング帯域は 1566〜1582 MHz に一致し，帯域幅やスペクトル形状はほぼ同一である一方，ポート間で最大数十 dB 程度の出力差が存在する結果となった。

1.2〜1.62 GHz の範囲で測定した広帯域スペクトルより，ポート 1〜ポート 3 では L1 帯以外の周波数において顕著な妨害成分は観測されず，ノイズフロア近傍のレベルにとどまることが確認された。すなわち，これらポート 1 から 3 は主として L1 帯単独のジャミング信号を出力していると解釈できる。

一方，ポート 4 では挙動が大きく異なった。図 4.5 はポート 4 の送信スペクトルを表したものである。

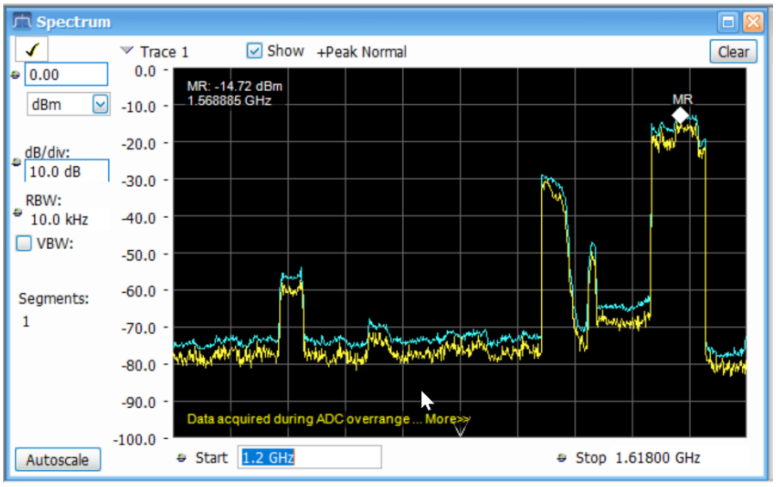


図 4.5　ジャマー：ポート 4 の送信スペクトル

ポート 4 を選択した場合，同じ 1.2〜1.62 GHz の測定範囲内で，L1 帯に加えて複数の周波数帯においてノイズフロアから大きく突出した成分が観測された。これらの成分は，いずれも数十 dB 程度ノイズフロアを上回るレベルであり，ポート 4 が L1 帯のみならず，他の GPS 関連周波数帯を含む広帯域のジャミング信号を同時に出力していることを示している。

4.2　スプーファーによる実験

スプーファーについてはソフトウェア上で GNSS の模擬信号を作成するが、このソフトウェアは中部大学の海老沼拓史教授が開発したオープンソースの GPS 信号シミュレータ LimeGPS をスプーファーとして利用するために改造したものである。

4.2.1 実験対象と使用機器

本節では，GNSS スプーフィングの成立可否を確認するために用いたスプーファーおよび受信機について述べる。送信側には，LimeSDR-USB と GNSS 再放射アンテナ，および GPS シミュレータソフトウェア LimeGNSS から構成される LimeGNSS スプーファーを用いた。LimeGNSS は中部大学海老沼研究室が作成したオープンソース GPS シミュレータを基に改良したソフトウェアであり，PC 上で任意の軌跡や静止位置に対応した GPS L1 C/A，QZSS L1C/A 信号を生成し，LimeSDR へ出力することで擬似衛星信号を送信することができる。

4.2.2　実験方法

(1) 機器構成

スプーフィング実験に用いた機器構成を図 4.6 に示す。PC と LimeSDR-USB は USB ケーブルで接続し，PC 上で動作する LimeGNSS により生成されたベースバンド I/Q データを LimeSDR に送信する。LimeSDR の RF 出力には LTE 用アンテナまたは GNSS-3P 再放射アンテナを接続し，GPS L1 帯の擬似衛星信号を空間放射した。

スプーファーからの電波が外部の GNSS 受信機に漏洩しないよう，PC・LimeSDR・アンテナおよび受信機は電波暗室またはシールドボックス内に設置した。スマートフォン 1,2 はスプーファー用アンテナの近傍（数十 cm 程度）に配置し，LimeGNSS スプーファーからの信号のみを主として受信するようにした。受信機から出力される位置・高度・時刻情報は，スマートフォン 1,2 の GNSS 地図アプリを用いて記録した。市販受信機 1 に関してはコンバイナーを使用して有線で真正信号とスプーフィング信号を混ぜながら受信機に注入した。こちらも位置・高度・時刻情報は市販受信機 1 のログ機能を用いて記録した実験機材と実験構成図を表 4.1 と図 4.6 に示す。

表 4.1　実験機材

名称	メーカー/型番
スマホ1	Xiaomi/Redmi12-5G
スマホ 2	Apple/iPhone14
受信機 1	u-blox/EVK-M8T
スプーファー	LimeSDR　USB
パッチアンテナ	u-blox/ANN-MB-00-00
送信アンテナ	LTE Antenna
コンバイナー	GPSNetworking/CPDC2X1-T

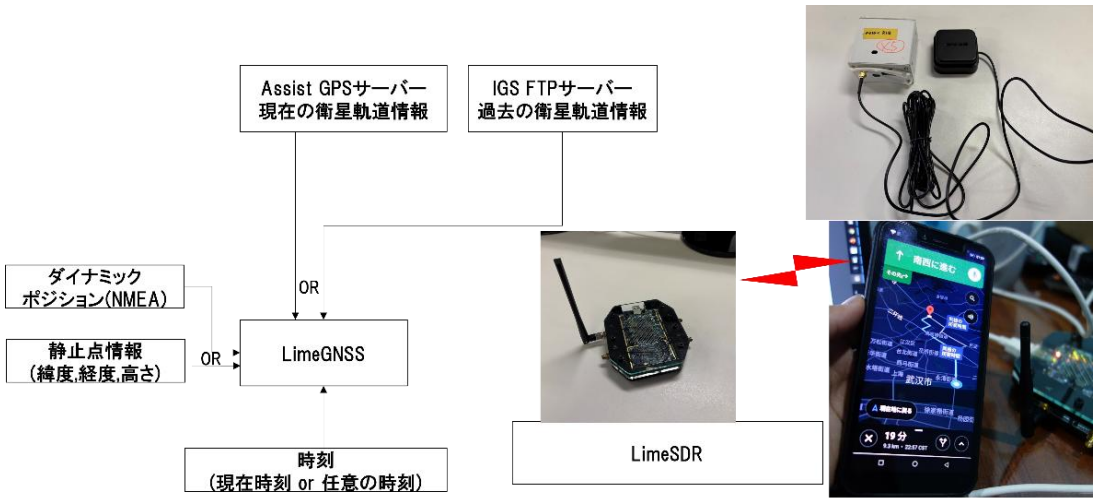


図 4.6　実験構成図

(2) 測定条件および手順

LimeGNSS の送信周波数は GPS L1 帯の 1575.42 MHz に設定し，帯域幅は 12 MHz とした。信号形式は GPS L1 C/A および QZSS L1C/A に対応させ，最大 16 チャンネルまで同時に擬似衛星信号を生成できる設定とした。送信電力は，受信機が飽和しない範囲で十分な受信 C/N0 が得られるよう，LimeSDR の出力設定値とアンテナ間距離により調整した。

実験手順を以下に示す。

1. 基準測位の取得

   スプーファーを停止した状態で，市販受信機およびスマートフォンを第 4 実験棟屋上に設置し，通常の衛星信号による測位を数分間行う。この測位結果を基準位置とする。

2. シールド環境での測位不能確認

   受信機を電波暗室／シールドボックス内に移動し，外部衛星信号を遮断した状態で測位を試みる。このときスプーファーは停止させておき，両受信機が衛星を捕捉できず「測位不能」と表示されることを確認する。

3. スプーフィング信号の印加

   LimeGNSS に欺瞞位置(都庁前：35.689507, 139.691728, 50.0)を設定し，指定した時刻から擬似衛星信号の送信を開始する。送信開始後，市販受信機およびスマートフォンが再び測位を開始するかどうかを観測し，位置・高度・時刻・捕捉衛星数などを一定時間ごとに記録する。

   市販受信機である u-blox の f9p においては、屋上の衛星を捕捉して、その情報を保持した状態からスプーフィング信号を受信するオーバーテイクと電波暗室内で受信機の内部情報をリセットしてスプーフィング信号を受信するコールドスタートのパ 2 つのパターンで記録する。

4. スプーフィングの判定
   受信機が測位不能状態から復帰し，表示される位置が基準位置から大きく逸脱した場合，または LimeGNSS で設定した仮想位置に一致して変化する場合をスプーフィング成功と判定する。

4.2.3 実験結果

まずは Xiaomi/Redmi12-5G のスプーフィング前後の地図上位置を図 4.7 に示す。

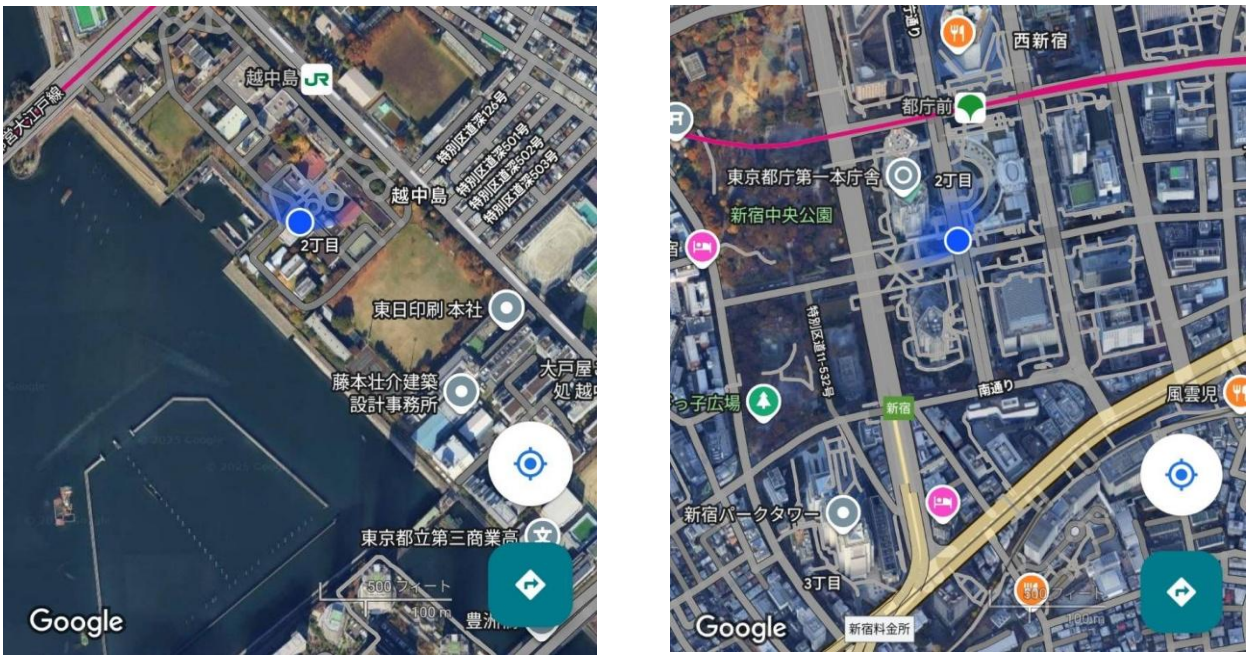


図 4.7　スマホ（Xiaomi）スプーフィング前（左）とスプーフィング後（右）の位置情報

スプーフィング信号を照射し始めて 25 秒で受信機の位置を欺瞞することに成功した。また、アプリの GPS logger を使用して受信されている衛星を可視化したものが図 4.8 である。
LimeGNSS の設定どおり GPS と QZSS の信号のみが生成されていることが分かる。

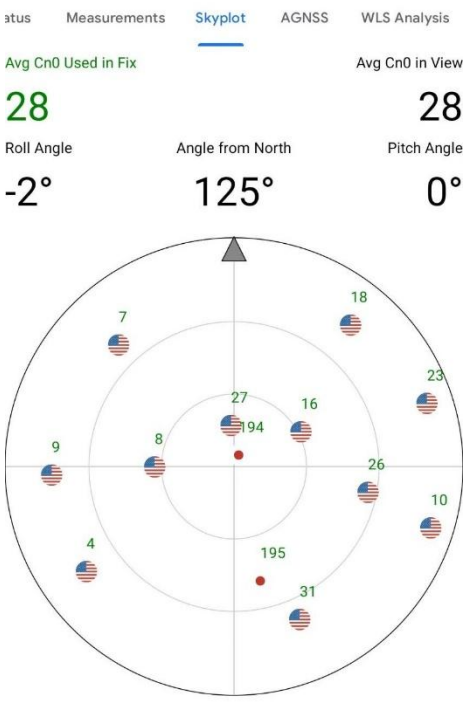


図 4.8　観測衛星図

次に Apple/iPhone14 のスプーフィング前後での位置情報を図 4.9 に示す。

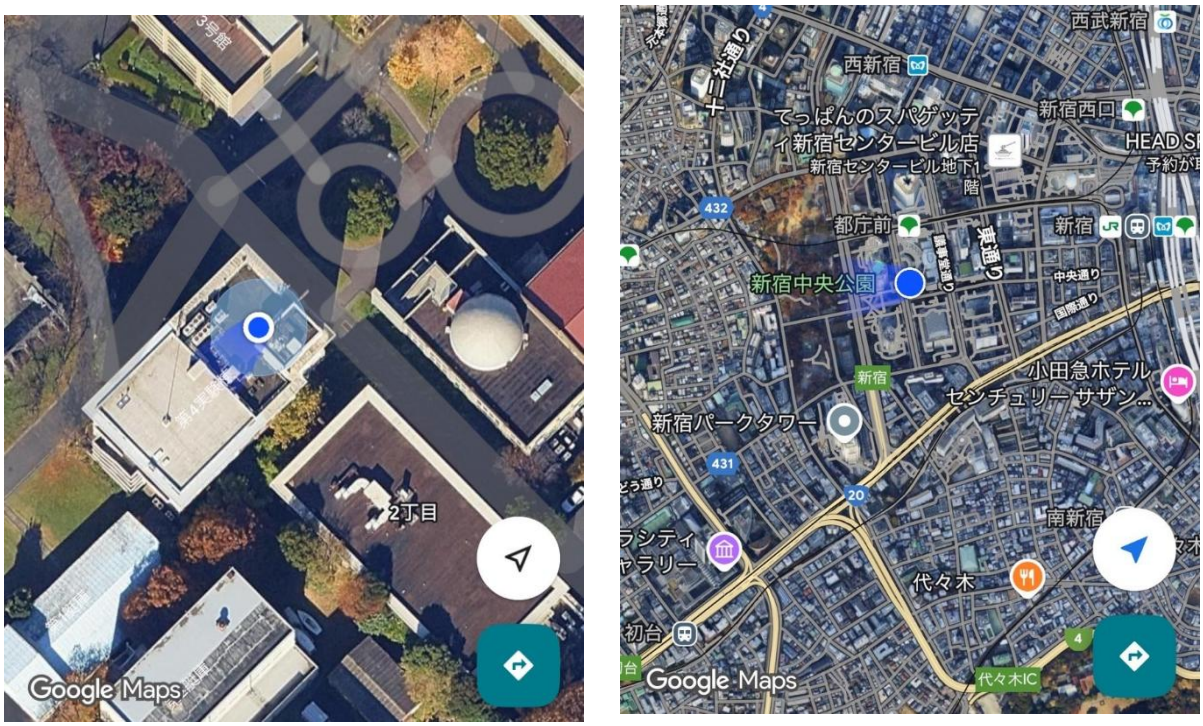


図 4.9　スマホ（iPhone）スプーフィング前（左）とスプーフィング後（右）の位置情報

iPhone も Xaomi 同様、スプーフィング信号を放射し始めて 54 秒で位置が都庁前へと移動した。このことからスマートフォンにおいてはメーカー間で GNSS の脆弱性に大きな差はないことが分かる。

最後に市販受信機へスプーフィングを行ったときの挙動を示す。図 4.10 と図 4.11 はオーバーテイクとコールドスタートの結果を u-center というアプリケーションで確認したものである。

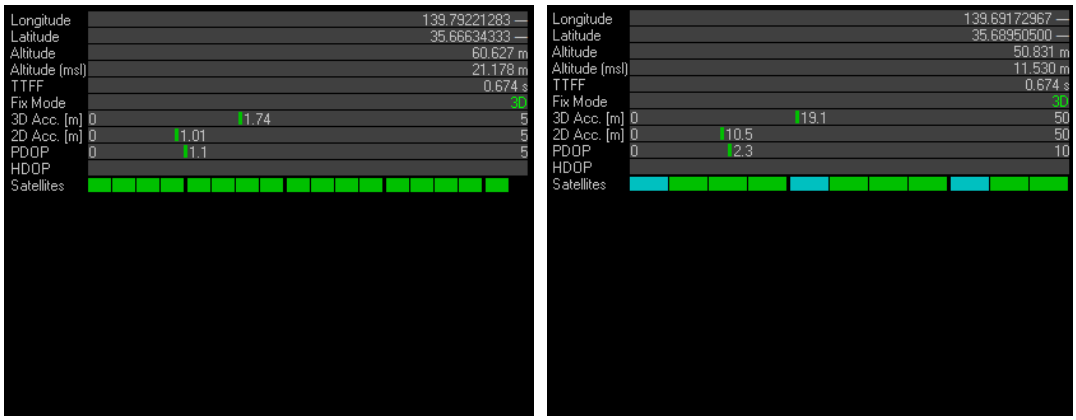


図 4.10　オーバーテイクでの受信機位置情報
スプーフィング前（左）スプーフィング後（右）

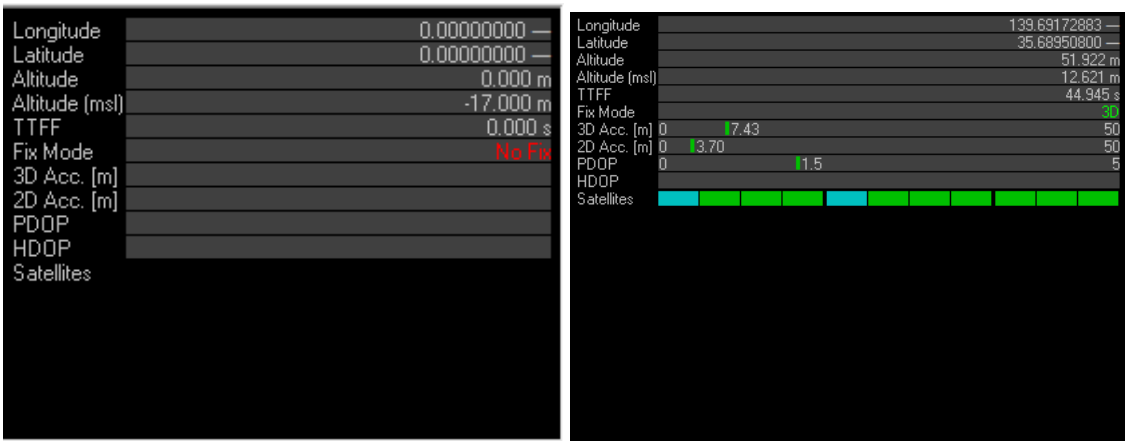


図 4.11　コールドスタートでの受信機位置情報
スプーフィング前（左）スプーフィング後（右）

オーバーテイクではスプーフィング信号を放射してから 1 分 50 秒で受信機の位置が都庁前へと移動した。一方でコールドスタートでは受信機の位置情報が欺瞞位置である都庁前で測位されるまで 47 秒かかった。コールドスタートは受信機の状態を初期化して追尾を始めるので、強いスプーフィング信号をしか受信できずすぐに間違った位置へと誘導されてしまう。一方でオーバーテイクの方は真正信号を追尾した状態から始まるため、スプーフィング信号によって一度測位不能状態にしてから偽の位置へ誘導しなくてはいけない。そのためスプーフィングにより長い時間がかかってしまう。

第5章　観測ドップラと予測ドップラによる

スプーフィング検知

この章では GNSS 衛星からの信号を受信した際に観測されるドップラ周波数を用いることで、スプーフィングを検出する手法を提案する。

5.1 ドップラ残差の RAIM

RAIM(Receiver Autonomous Integrity Monitoring)とは、受信機が自律的に測位結果の健全性を監視し、異常が疑われるときに検出して警報を出す仕組みです。衛星測位によって PVT(Position, Velocity, Timing)を推定した時に、その PVT と衛星のエフェメリスを用いることで観測することのできるドップラ周波数を予測することが可能である。スプーフィング信号と衛星からの正しい信号が混在している場合、ドップラ測位による PVT 解が歪むため、観測ドップラと PVT から生成した予測ドップラの差分に変化が現れる現象を利用した RAIM によってスプーフィングの検知手法を提案した。

5.2　ドップラ周波数の概要

ドップラ効果とは、送受信機間の相対運動により受信される信号の周波数が送信周波数からずれる現象のことである。この時の周波数偏移をドップラ周波数と呼ぶ。GNSS では、衛星から送信される搬送波の中心周波数が決まっているため、受信機が信号を追尾する過程でこの周波数のずれを推定することができる。

送受信の周波数(Hz)をf_T、f_Rとして、$\dot{r}$は送受信機関の距離(m)、cを信号の伝搬速度(m/s)とすると送信周波数と受信周波数には次のような関係が成り立つ。

$$f_R = f_T\left(1 - \frac{\dot{r}}{c}\right) \tag{5.1}$$

5.3　ドップラ測位の概要

受信機が信号追尾で推定した公称周波数からのずれは、衛星—受信機間の相対運動によるドップラシフトを主成分として含むため、衛星と受信機の相対速度（視線方向速度）を観測していると解釈できる。この性質を利用し、複数衛星のドップラを同時に用いることで、受信機の三次元位置、速度と受信機時計ドリフト（周波数基準のずれ）を推定できる。衛星の位置・速度は暦情報から計算できるため、受信機側の未知量は「受信機がどの方向にどれだけ動いているか」と「受信機の発振器がどれだけずれているか」に集約され、衛星数が十分あれば幾何学的に解ける。

ここからはドップラ測位の観測モデルを説明する。

衛星 i と受信機間の観測ドップラD_i^{obs}を次のように定義する。

$$D_i^{obs} = f_i - f_r \tag{5.2}$$

f_i：衛星 i から送信された搬送波周波数(Hz)

f_r：受信機で受信された周波数(Hz)

このとき受信機から衛星 i への視線ベクトル$\mathrm{e_i}$は、衛星 i の位置r_iと受信機の位置r_rを用いて

$$e_i = \frac{r_i - r_r}{\|r_i - r_r\|} \tag{5.3}$$

相対速度の LOS(Line of Sight)成分$\dot{\rho}_i$は次のように定義できる。

$$\dot{\rho}_i = e_i \cdot (v_i - v_r) \tag{5.3}$$

ρ_i：衛星 i と受信機の擬似距離(m)

v_i：衛星 i の速度(m/s)

v_r：受信機の速度(m/s)

搬送波は光速で伝搬するので擬似距離変化率$\dot{\rho}_i$と観測ドップラには以下の関係が成り立つ。

$$D_i^{obs} = -\frac{f_i}{c}\dot{\rho}_i \tag{5.4}$$

衛星 i と受信機間の観測ドップラのモデル式で表す。

$$D_i^{model} = -\frac{f_i}{c} e_i \cdot (v_i - v_r\,) + \dot{\delta}t \tag{5.5}$$

観測残差は次の式で表される。

$$\begin{aligned} z_i &= D_i^{obs} - D_i^{model} \\ &= D_i^{obs} - \left(-\frac{f_i}{c} e_i \cdot (v_i - v_r) + \dot{\delta}t\right) \end{aligned} \tag{5.6}$$

ドップラ測位における未知量は受信機位置(x, y, z),受信機速度(v_x, v_y, v_z),クロックドリフト$\dot{\delta}t$である。このとき推定すべき状態ベクトルは次のようになる。

$$x = \begin{bmatrix} x & y & z & v_x & v_y & v_z & \dot{\delta}t \end{bmatrix}^{\mathsf{T}} \tag{5.7}$$

観測モデルは非線形なのである近似値x_0周りで線形化すると

$$z_i \approx H_i\,\Delta x \tag{5.8}$$

ここでΔxは未知量と近似値の残差を表す。

$$\Delta x = x - x_0 \tag{5.9}$$

H_iは衛星 i に対するヤコビアン行列の 1 行で

$$H_i = \left[\frac{\partial D_i^{model}}{\partial x} \quad \frac{\partial D_i^{model}}{\partial y} \quad \frac{\partial D_i^{model}}{\partial z} \quad \frac{\partial D_i^{model}}{\partial v_x} \quad \frac{\partial D_i^{model}}{\partial v_y} \quad \frac{\partial D_i^{model}}{\partial v_z} \quad \frac{\partial D_i^{model}}{\partial \dot{\delta}t}\right]_{x=x_0} \tag{5.10}$$

速度とクロックドリフトに関する偏微分を行う。

$$\frac{\partial D_i^{model}}{\partial v_r} = -\frac{f_i}{c}\frac{\partial}{\partial v_r}[e_i^{\top}(v_i - v_r)] = \frac{f_i}{c}e_i \tag{5.11}$$

速度はx, y, z各成分について偏微分を行う。

$$\frac{\partial D_i^{model}}{\partial v_x} = \frac{f_i}{c}e_{ix},\ \frac{\partial D_i^{model}}{\partial v_y} = \frac{f_i}{c}e_{iy},\ \frac{\partial D_i^{model}}{\partial v_z} = \frac{f_i}{c}e_{iz} \tag{5.12}$$

クロックドリフトについて偏微分を行う。

$$\frac{\partial D_i^{model}}{\partial \dot{\delta} t} = 1 \tag{5.13}$$

擬似距離のレンジレート(m/s)は

$$\dot{\rho}_i = e_i \cdot (v_i - v_r) \tag{5.13}$$

これを受信機位置r_rで偏微分すると

$$\frac{\partial \dot{\rho}_i}{\partial r_r} = -\frac{v_i - v_r}{\|r_i - r_r\|} + \frac{(r_i - r_r) \cdot (v_i - v_r)}{\|r_i - r_r\|^3}(r_i - r_r) \tag{5.14}$$

観測モデルで同様の偏微分を行ったとき

$$\frac{\partial D_i^{model}}{\partial r_r} = -\frac{f_i}{c}\frac{\partial \dot{\rho}}{\partial r_r} \tag{5.15}$$

(5.14)と(5.15)からx, y, z各成分の偏微分を求める。

$$\begin{aligned}
\frac{\partial D_i^{model}}{\partial x} &= \frac{-f_i}{c\|r_i - r_r\|}(v_{ix} - v_x - \dot{\rho}_\iota e_{ix}) \\
\frac{\partial D_i^{model}}{\partial y} &= \frac{-f_i}{c\|r_i - r_r\|}(v_{iy} - v_y - \dot{\rho}_\iota e_{iy}) \\
\frac{\partial D_i^{model}}{\partial z} &= \frac{-f_i}{c\|r_i - r_r\|}(v_{iz} - v_z - \dot{\rho}_\iota e_{iz})
\end{aligned} \tag{5.16}$$

したがって衛星 i に対するヤコビアン行列を求めることができる。
これを全衛星について並べたものが、観測に対するヤコビアン行列 H となる。
衛星数をnとし、観測残差ベクトルと観測ベクトルを

$$z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix},\ y = \begin{bmatrix} D_1^{obs} \\ D_2^{obs} \\ \vdots \\ D_n^{obs} \end{bmatrix} \tag{5.17}$$

としたとき、線形化された観測方程式を求める。

$$z = y - D^{model}(x_0) \approx H\Delta x \tag{5.18}$$

重み行列Wとしたとき、観測モデルと推定値の残差は次のようになる。

$$\Delta x = (H^{\top}WH)^{-1}H^{\top}Wz \tag{5.19}$$

現在の推定値x_{old}に真値への未知量Δxを足すことで新たな推定値x_{new}へ更新する。

$$x_{new} = x_{old} + \Delta x \tag{5.20}$$

この更新が収束するまで繰り返すことでドップラ観測寮から受信機の 3 次元位置・ 3 次元速度・クロックドリフトを推定することができる。

5.4　予測ドップラの生成手法

衛星から送られてくるエフェメリスから求めた衛星位置とドップラ測位によって求めた受信機の PVT を用いることで、観測されるはずのドップラを予測する。

時刻 t（受信時刻t_{rx}）・衛星 i について予測ドップラの生成について定式化を行う。

文字は次のように定義する。

ECEF 座標系上での衛星位置・速度：$r_i(t),\ v_i(t)$

受信機位置・速度(ドップラ測位による PVT)：$r_r(t) = (x, y, z)^{\top},\ v_r = \left(v_x, v_y, v_z\right)^{\top}$

光速：$c = 299{,}792{,}458\, m/s$

搬送波周波数(GPS/QZSS/Galileo :L1/E1)：$f_i = 1575.42 \times 10^6\ Hz$

衛星のクロック参照時刻：t_{oc}

衛星クロック補正係数：a_{f_0}, a_{f1}, a_{f2}

基準時刻と受信時刻の時刻差(s)：$\Delta t = t_{oc} - t_{rx}$

衛星のクロックバイアス$dts(t)$とクロックドリフト$\dot{dts}(t)$は次のように求めることができる。

$$dts(t) = a_{f_0 +} a_{f_1} \Delta t + a_{f_0} \Delta t^2 \tag{5.21}$$

$$\dot{dts}(t) = a_{f_1} + 2a_{f_0}\ \Delta t \tag{5.22}$$

衛星のクロックドリフトは擬似距離のレンジレート次のように寄与する。

$$\dot{\rho}_i^{clk}\ (t) = -c\ \dot{dts}(t) \tag{5.23}$$

同様に受信機クロックドリフトの擬似距離レンジレートへの寄与を求める。

$$\dot{\rho}_r^{clk} = c\dot{\delta}t \tag{5.24}$$

衛星 i と受信機間の擬似距離$\rho_i(t)$は次のように求めることができる。

$$\Delta r_i(t) = r_i(t) - r_r(t)$$

$$\rho_i(t) = \|\Delta r_i(t)\| \tag{5.25}$$

LOS 単位ベクトルは、$\rho_i(t)$を用いて

$$e(t) = \frac{\Delta r_i(t)}{\rho_i(t)} \tag{5.26}$$

と表わすことができる。したがって衛星と受信機の幾何レンジレートは

$$\dot{\rho}_{i,geom}(t) = e_i(t)^{\top}\left(v_i(t) - v_r(t)\right) \quad [m/s] \tag{5.27}$$

となる。クロックドリフトと幾何を考慮したモデルレンジレートは

$$\dot{\rho}_i^{pred}(t) = e_i(t)^{\top}\left(v_i(t) - v_r(t)\right) + c\dot{\delta}t - c\ \dot{dts}(t) \tag{5.28}$$

以上から予測ドップラ周波数は次の式で表される。

$$f_i^{pred}(t) = -\frac{f_i}{c}\dot{\rho}_i(t)$$

$$f_i^{pred}(t) = -\frac{f_i}{c}\left[e_i(t)^{\mathrm{T}}\left(v_i(t) - v_r(t)\right) + c\dot{\delta}t - c\,\dot{dts}(t)\right] \tag{5.29}$$

5.5　評価実験 1

提案手法を評価するために、3 つの実験を行った。1 つ目は静止アンテナから真正信号のみを受信した場合の観測ドップラと予測ドップラの残差を確認しスプーフィングを検出するか評価した。

5.5.1　実験概要

実験は本大学の第 4 実験棟屋上の静止アンテナを用いて行った。受信機は Septentrio 社の mosaicX5 を使用した。実験構成図と使用機材の表をそれぞれ図 5.1 と表 5.1 に示す。

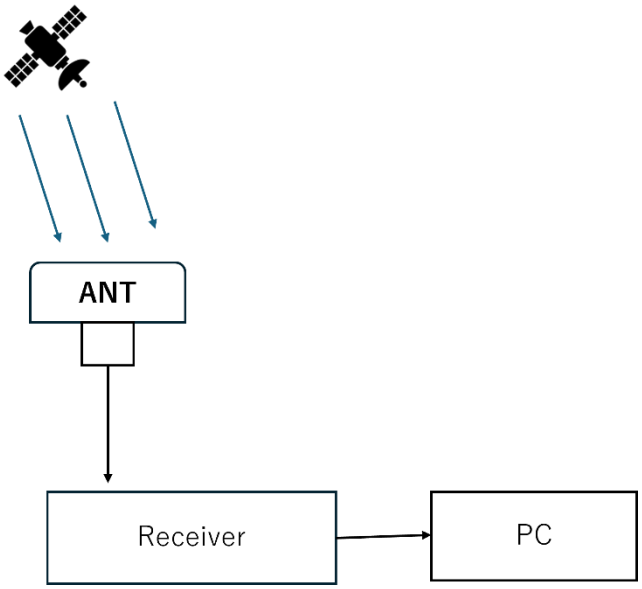


図 5.1　実験構成図

表 5.1 実験機材

名称	メーカー/型番
アンテナ	TOPCON CR-G5-C
受信機	Septentrio MosaicX5

今回の実験では GPS の L1 帯 QZSS の L1 帯、Galileo の E1 帯,E5 帯のみを 1Hz で受信機ログを取得するように設定した。これは衛星の機数が増えすぎてしまうと実験 2 ,3 でスプーフィングを

行った際にうまく信号を追尾できなくなるためである。ドップラ測位と予測ドップラの生成と RAIM は受信機から取得した rinex ファイルと nav ファイルを読み込んで実行するプログラムを Python で作成した。

5.5.2　実験結果 1

真正信号のみを観測した場合、ドップラ測位はすべての PVT で観測ドップラと予測ドップラの整合性が保たれているため残差はノイズレベルとなる。RAIM については同一衛星で予測ドップラと観測ドップラの残差が 1Hz 以上となるエポックが 30 以上連続で検出された場合にアラートを出すものとした。図 5.2 はスプーフィングアラートの結果を示している。ドップラ測位はすべての時間で行うことができた。また、図 5.3 は例として Galileo の E25 のドップラ残差を表したものである。

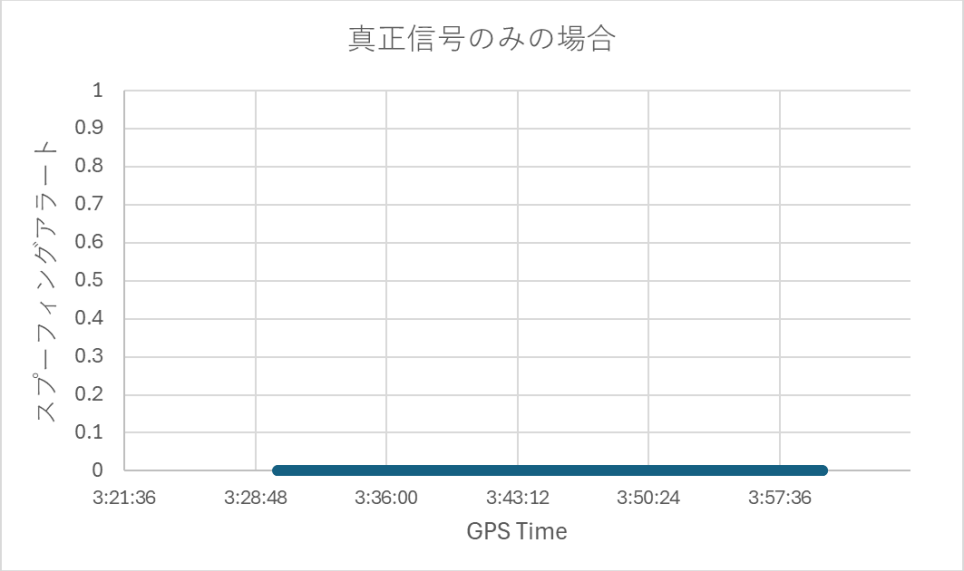


図 5.2　スプーフィングアラートの結果

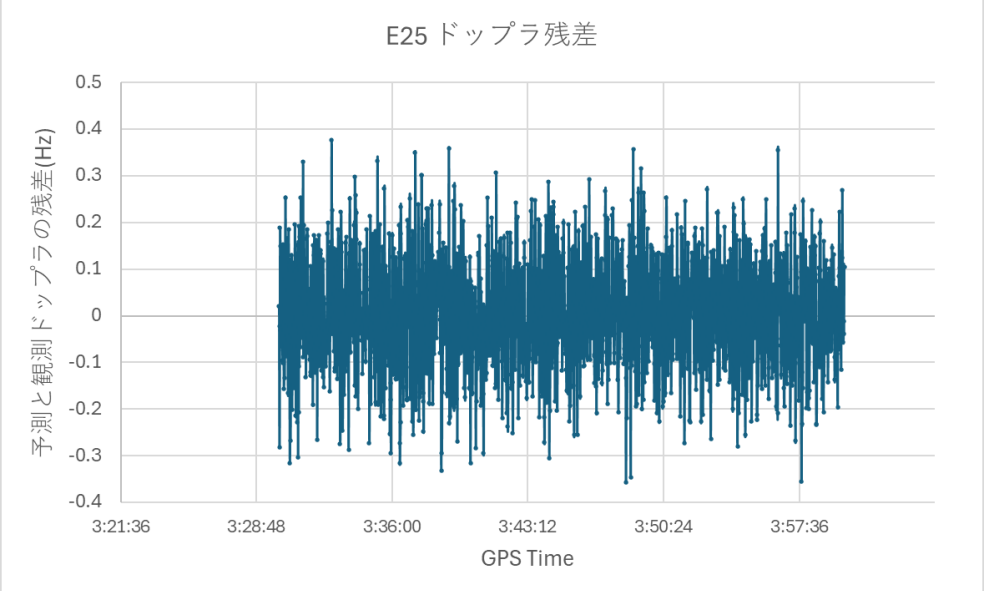


図 5.3　　Galileo E25 予測ドップラと観測ドップラの残差

20 分間のデータの中でスプーフィングアラートは一度も発生せず、誤検出はされなかった。これは真正信号のみでドップラ測位を行うと受信機の PVT 整合性がとれているため、予測ドップラと観測ドップラの残差がノイズレベルとなっていたためである。この実験は屋上の静止アンテナを使用しているため、移動体の受信機依存のドップラ周波数や衛星からのマルチパス信号が考慮されていない。

5.6　評価実験 2

2 つ目の実験はスプーファーから欺瞞信号のみを照射した場合にドップラ RAIM によってスプーフィングを検出できるのかを評価した。

5.6.1 実験概要

この実験は GNSS の妨害電波を空間放射してしまうので本大学第 4 実験棟 5 階にある電波暗室内で実験を行った。実験機材と実験構成図、実験風景写真を表 5.2 と図 5.4、図 5.5 に示す。

名称	メーカー/型番
アンテナ	u-blox ANN-MB-00-00
スプーファーアンテナ	LTE Antenna
受信機	Septentrio MosaicX5
スプーファー	LimeSDR USB

表 5.2　実験機材

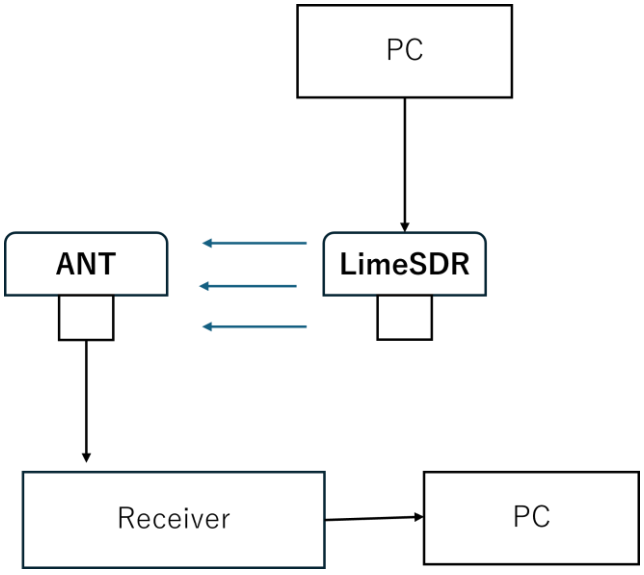


図 5.4　実験構成図

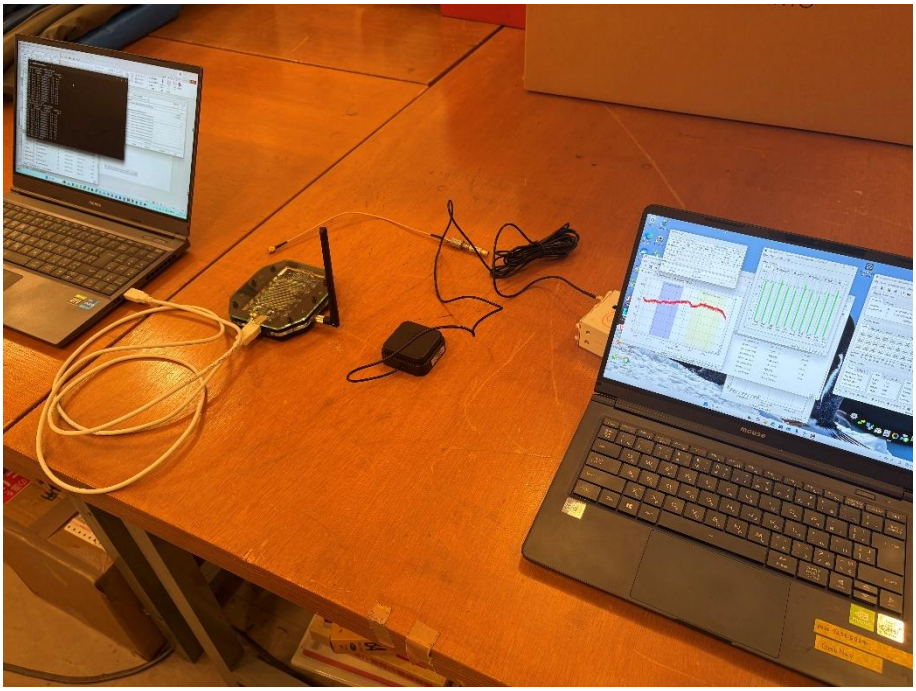


図 5.5　実験 2 風景図

LimeSDR は L1 帯の信号のみ生成できるため、この実験では GPS L1 帯と QZSS L1 帯の信号しか記録できていない。また、受信機が安定してスプーフィング信号を追尾することが難しく、この実験では 5 分間のデータを記録することができた。スプーフィングシナリオは図 5.6 に示すように東京湾を船速 10 ノット程度で航行するという内容で行った。

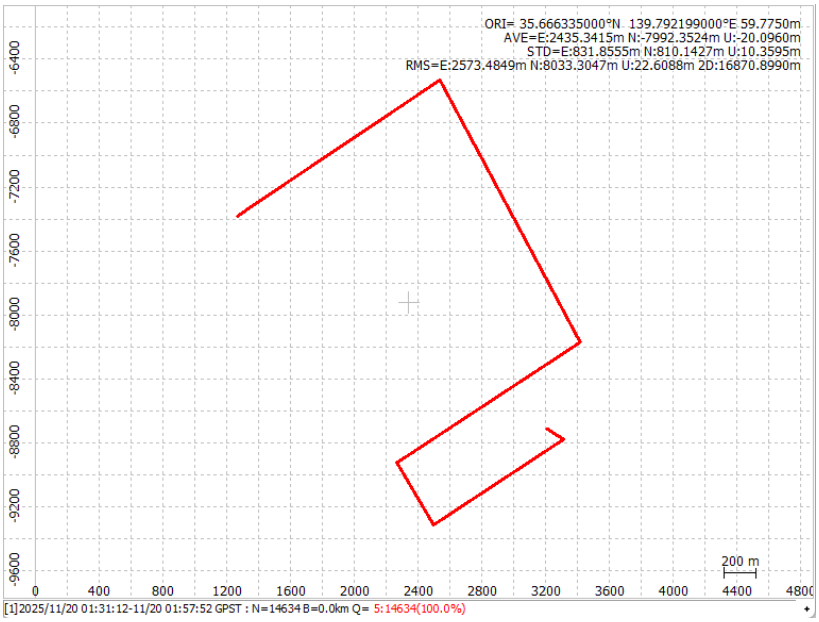


図 5.6　スプーフィングシナリオ

5.6.2　実験結果 2

スプーフィング信号のみを観測した場合のスプーフィングアラートの結果を図 5.7 に示す。

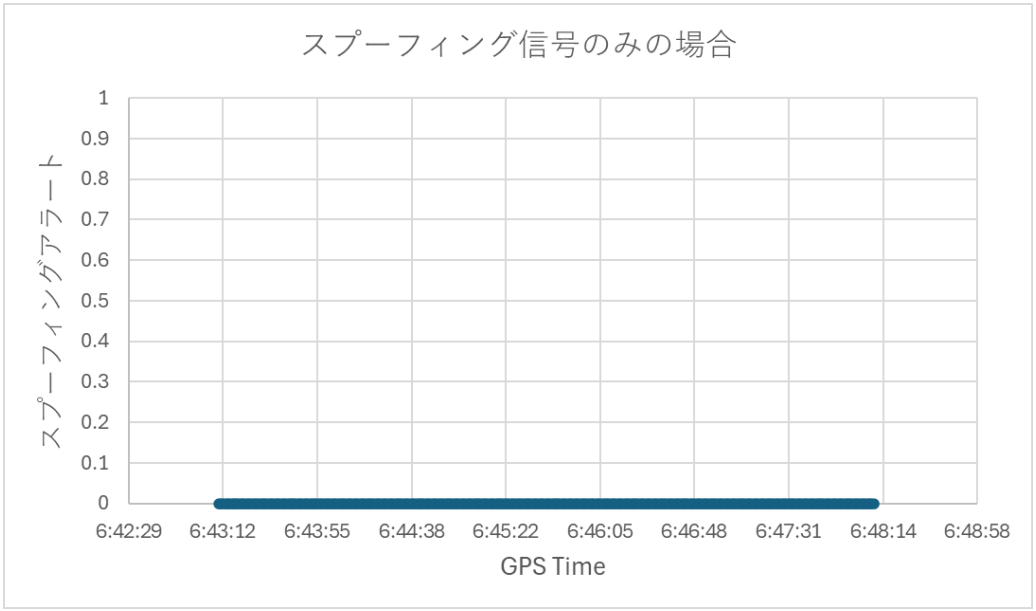


図 5.7　スプーフィングアラートの結果

この実験ではスプーフィングアラートは出されず、すべてのエポックでスプーフィングを見逃した。スプーフィング信号のみでドップラ測位を行った場合すべての偽の PVT で観測ドップラと予測ドップラの整合性が保たれる。結果として残差はノイズレベルとなり、スプーフィングは検出されなかったのだと予想される。GPS の G04 のドップラ残差の結果を例として図 5.8 に示す。

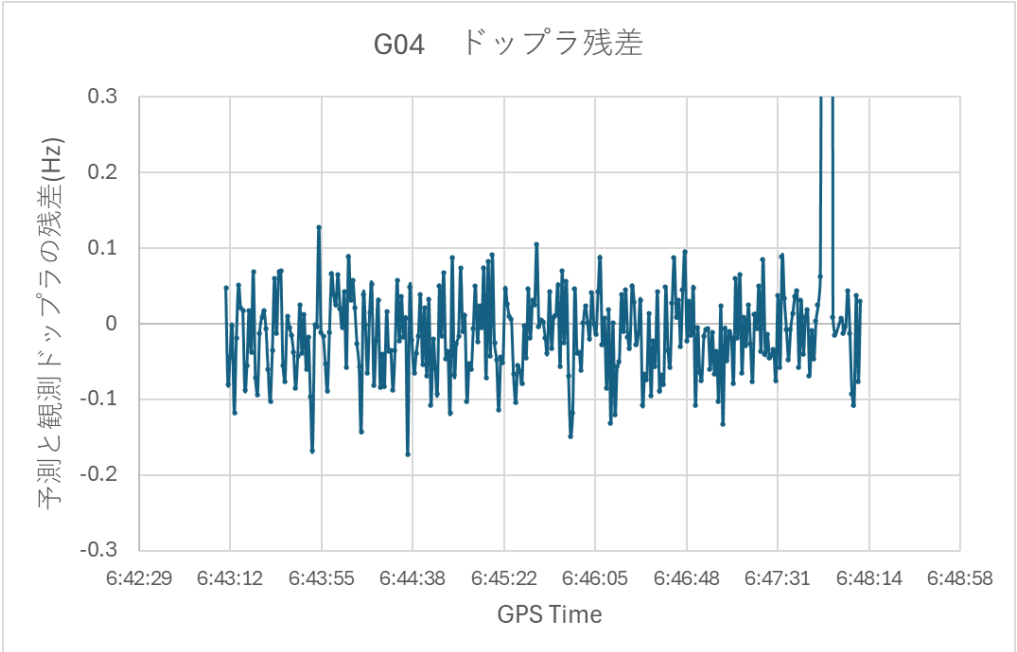


図 5.8　GPS G04 予測ドップラと観測ドップラの残差

G04 においては予測と観測ドップラの残差が約 0.1Hz から-0.2Hz の間を推移しているが、6:47:56 の 1 エポックだけ約 3.5Hz の残差となった。

5.7　評価実験 3

3 つ目の実験ではリアルの衛星信号とスプーフィング信号が混成して受信されたときに、スプーフィングを検出できるのかについて評価した。

5.7.1　実験概要

真正信号とスプーフィング信号を同時に追尾することが今回使用した受信機では困難だったため、2023 年に Fraunhofer から提供されたスプーフィングシミュレーションデータセットを用いてスプーフィングの検出を行うことができるのか検証した。図 5.9 はスプーフィングシナリオを示す。

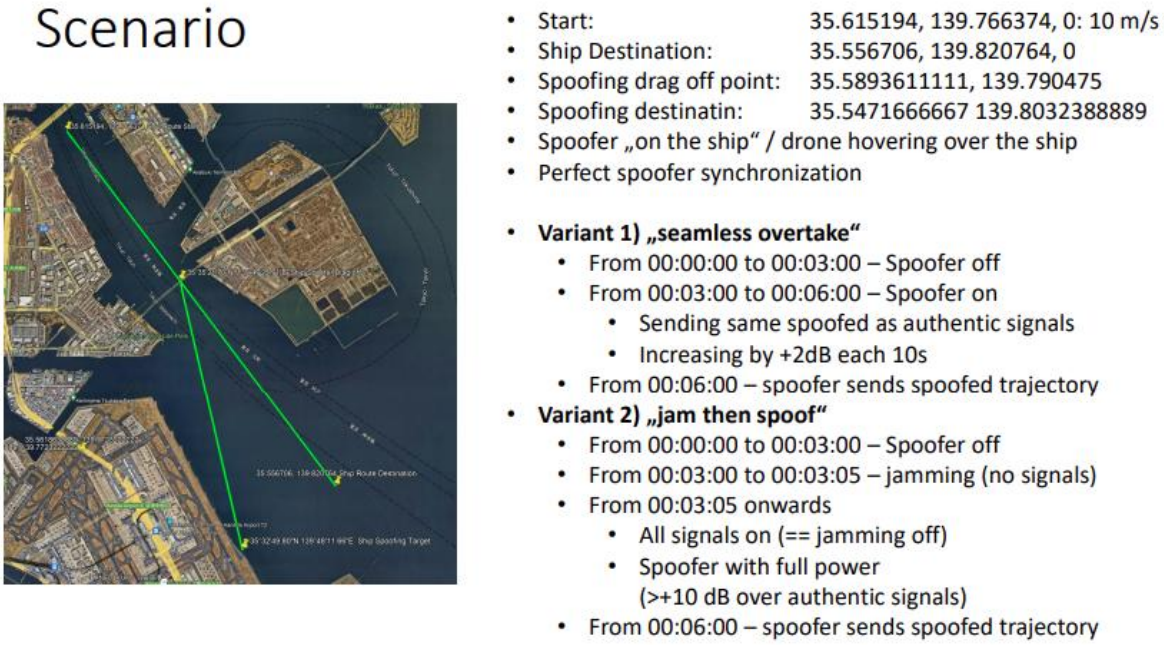


図 5.9　スプーフィングのシナリオ

使用したのは seamless overtake のシナリオで、東京湾を航行する船へのスプーフィングを想定している。00:02:30 からスプーフィングを開始し、00:06:00 から欺瞞位置に誘導する。欺瞞位置への誘導を開始する前は受信機と同じ位置のスプーフィング信号を信号強度を徐々に強めながら送信する。データセットは実験 1，2 と同様に 1 Hz で受信機ログを取得している。このデータセットでは GPS と QZSS の L1 帯のみを記録している。また GPS 信号のみをスプーフィングしており、QZSS の信号は常に真正信号が追尾されている。

5.7.2　実験結果 3

シミュレーションデータセットを用いてドップラ測位を行い、観測ドップラと予測ドップラの残差による RAIM を行った。図 5.10 はスプーフィングアラートの結果を示している。

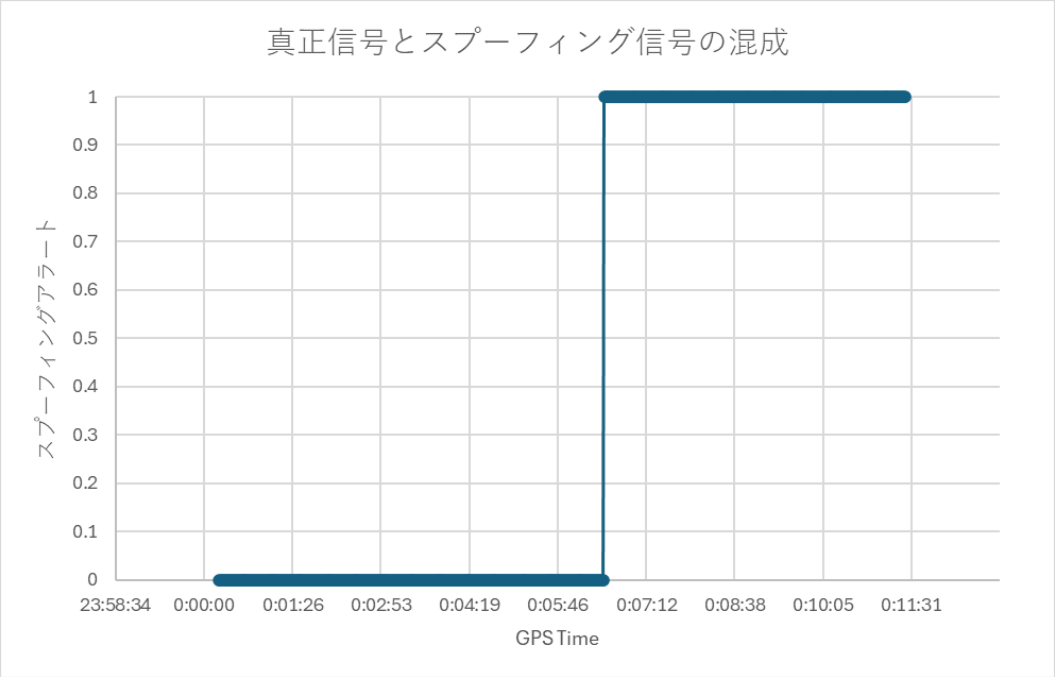


図 5.10　スプーフィングアラートの結果

RAIM では 00:06:31 からデータの取得が終了する 00:11:25 までスプーフィングアラートが出た。このため RAIM による誤検出率は 0 %であったが、スプーフィングを開始してから 270 エポック、位置の欺瞞を開始してから 30 エポックはスプーフィングを見逃していた。そのため見逃し率はそれぞれ 47.8%と 5.3%となっている。

GPS と QZSS それぞれでドップラ残差がどのように変動しているか、GPS の G12 と QZSS の J04 の結果を例として図 5.11 に示す。

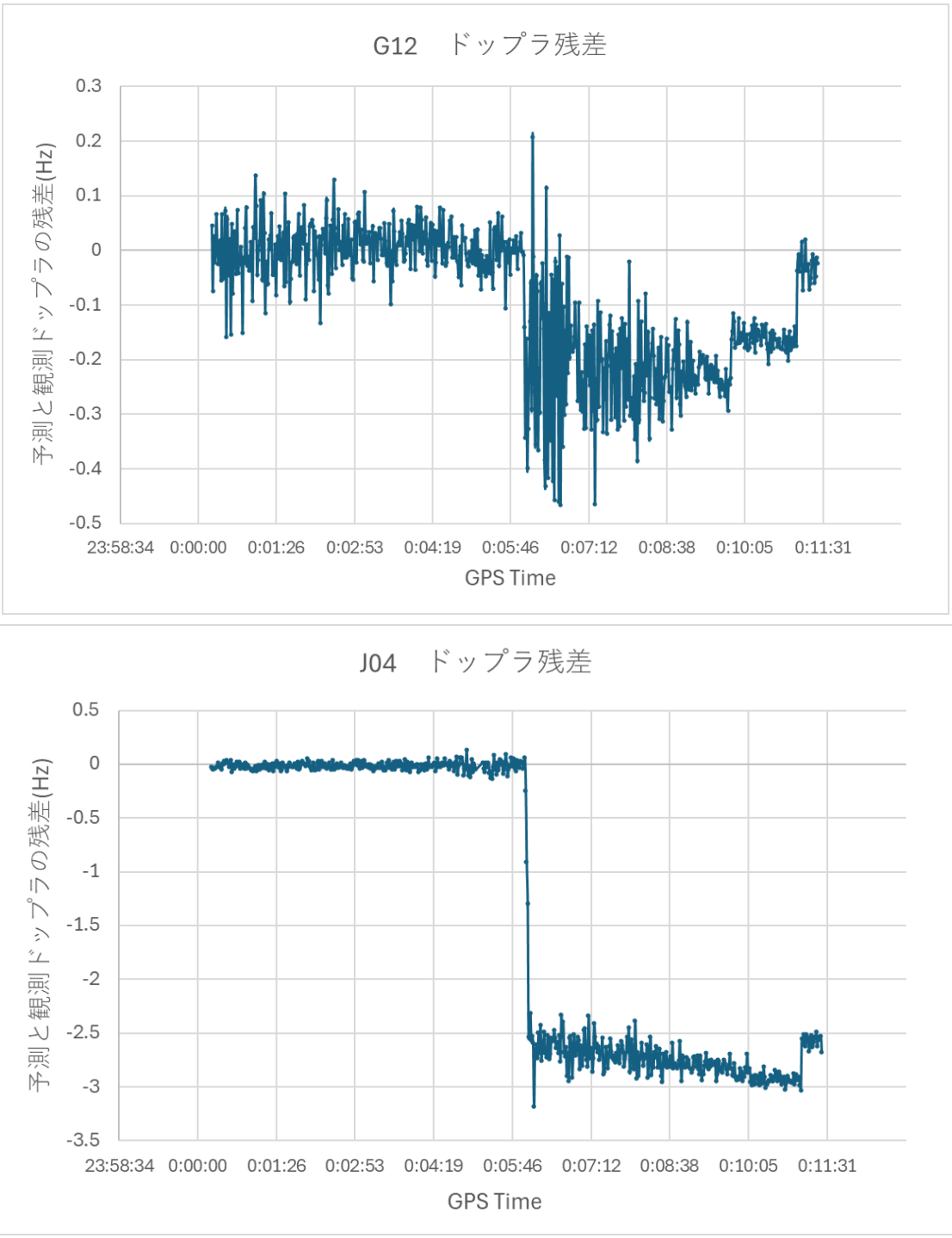


図 5.11　GPS G12 と QZSS J01　予測と観測ドップラの残差

どちらの衛星も欺瞞位置への誘導が開始した 00:06:00 からドップラの残差が大きくなっている。特に、真正信号を追尾している QZSS はドップラ残差が 1 Hz 近く出ている。

第6章　結論

この章では行った実験結果から提案手法によるスプーフィング検知の可用性の考察や本研究のまとめ、今後の展望についてまとめる。

6.1　スプーフィング検知実験の考察

表 6.1 は各実験結果を表したものである。受信する信号の種類は実験 1 が真正信号のみ、実験 2 がスプーフィング信号のみ、実験 3 が真正信号とスプーフィング信号の混成となっている。

表にはドップラ測位を行った測位回数（Total Epoch)、スプーフィングアラートが出たエポック（Spoofing detection Epoch)、スプーフィングの見逃し率、スプーフィングの誤検出率をまとめた。

図 6.1　実験結果比較図

	実験1	実験2	実験3
Total Epoch	1800	302	671
Spoofing detection Epoch	0	0	295
見逃し率	0.0%	100.0%	47.8%
誤検出率	0.0%	0.0%	0.0%

実験 1 の結果より、受信する信号が真正信号のみであれば、各衛星からのドップラは常に整合性を保つためスプーフィングの誤検出がなされないことが分かる。ただし、本実験はオープンスカイの静止アンテナで行っているため、都市部の移動体といったマルチパスが非常に多い環境での可用性を担保できていない。実験 2 ではスプーフィング信号のみを受信したが、スプーフィングを検出することができなかった。これはスプーファーから放射される信号のドップラが衛星ごとに整合性のとれるように調整されているためだと推察される。このため、提案した手法では高価なスプーファーによる全衛星の乗っ取りは検知できないと考えられる。実験 3 ではスプーフィングを開始してから 270 エポック、位置の欺瞞を開始してから 30 エポックはスプーフィングを見逃していた。そのため見逃し率はそれぞれ 47.8%と 5.3%となっている。真正信号とスプーフィング信号の欺瞞位置が一致している間はスプーフィングを検出できない。しかし、欺瞞位置への誘導が開始されると各ドップラの整合性が取れず、ドップラ測位解が歪むことからスプーフィングによる検出が可能になることが推察できる。

6.2　本研究の総括と今後の展望

本研究ではジャミング、スプーフィングによる事故事例や実際の機器を用いた出力調査によって、年々高度化する GNSS 妨害手法を把握することができた。

一方で、高度化する妨害手法に対して検出手法や防御策の研究がどのように行われているかを調査した。それぞれの防御手法は「守る対象」と「介入する階層（レイヤ)」が異なるため、同じ尺度で評価することはできなかったが、手法ごとに長所と短所が存在し、それらを組み合わせることでより強固な防御策へと昇華できると考えられる。

観測ドップラと予測ドップラの残差によるスプーフィング検知手法は安価なスプーファーによる 1 つの GNSS 信号帯域のみの欺瞞であれば検知することができた。しかし、実験 3 はあくまでシミュレーションデータで RAIM を行っただけであり、実環境でのデータは取得できていない。また、閾値に関しても

最後に今後の課題を述べる。ジャマーとスプーファーの評価に関してはより高性能なジャマー、スプーファーの出力と挙動の確認や、受信機メーカーごとの測位システム評価を行いたい。

スプーフィング検出実験では電波法の関係で広範囲でのスプーフィング実験ができなかった。屋外の移動体に対するスプーフィング攻撃を再現するためには、ドイツのベルヒテスガーデンのように正式に許可をとって実験を行うほかない。また、兵庫県赤穂市にジャミングやスプーフィングなどの電波干渉実験をオープンフィールドで行える実験試験局が存在するが、大学等の研究機関による実験は制限されている。さらに、海上での電波実験は国際水域上で低出力かつ科学的な範囲で行うことができる。たとえば、本学が所持する汐路丸が国際水域上を航行する際に、電波法の定める電界強度以下でスプーフィング実験を実施することは問題ない。今後、国内に実験制限のない実験試験局が開設され電波干渉対策がより進展することに期待したい。

本研究では検知までを行ったが将来的には検知後に代替の測位システムで正常な測位を継続していくことが目標であるため、今後はスプーフィング検知と並行して GNSS に依存しない位置測位継続システムの研究にも着手する必要があると思われる。

参考文献

1. Ziheng Zhou , Hong Li , and Mingquan Lu. (2025)
   Doppler-Based RAIM for GNSS Spoofing Detection in Vehicular Applications
2. Mark L. Psiaki and Todd E. Humphreys (2016)
   GNSS Spoofing and Detection
3. Chuhan Huang , Fan Feng, Chufeng Duan, Zhengkun Chen, Pengrui Mao, Xuelin Yuan, Xiangwei Zhu (2025)
   To lock the authentic signals: mitigating GNSS spoofing with INS-aided tracking
4. 小林海斗（2021）
   GNSS スプーフィングの検知手法の研究
5. 芝田，淳之介，辻井，利昭，藤原，健，大澤，壮志（2024）
   スプーフィング検知に向けた MUSIC 法による信号到来方向推定 DOA Estimation of GNSS Signals for Spoofing Detection Based on the MUSIC Algorithm
6. 奥富 雄司（2024）
   GNSS 妨害の低減手法の研究
7. Reuters (2025/2/4)
   Crashed Azerbaijani plane was riddled with holes after incident over Russia, report says
   https://www.reuters.com/world/asia-pacific/kazakh-report-says-plane-dec-25-crash-probably-damaged-by-external-objects-2025-02-04/
8. Sam Chambers (2025)
   Grounded MSC ship appears in the Sahara (2025/5/20)
   https://splash247.com/grounded-msc-ship-appears-in-the-sahara/
9. The European Union Aviation Safety Agency (2025/1/9)
   CZIB No.: 2025-01Subject: Airspace of the Russian Federation
10. Federal Aviation Administration (2025/12/04)
    Jamming and/or Spoofing/GNSS Interference Resource Guide/FLIGHT TECHNOLOGIES AND PROCEDURES DIVISION
11. Inside GNSS (2025/7/24)
    Galileo Leads the Way in GNSS Spoofing Protection with OSNMA
    https://insidegnss.com/galileo-leads-the-way-in-gnss-spoofing-protection-with-osnma/
12. Inside GNSS (2025/7/8)
    Swift Navigation Skylark™ Precise Positioning Service: Defending Against Spoofing with GNSS Corrections
    https://insidegnss.com/defending-against-spoofing-with-gnss-corrections/

13. Inside GNSS (2025/5/15)
MSC Antonia Grounding in the Red Sea Attributed to Suspected GNSS Spoofing
https://insidegnss.com/msc-antonia-grounding-in-the-red-sea-attributed-to-suspected-gps-spoofing/
14. 長岡 賢吾（2023）
2 つのアンテナを用いた GNSS スプーフィング検知手法の研究