一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
SANE2018-33（2018-08）

GPS のセキュリティ：脆弱性とその対策

坂井 丈泰†

†国立研究開発法人海上・港湾・航空技術研究所電子航法研究所
182-0012 東京都調布市深大寺東町 7-42-23
E-mail: †sakai@mpat.go.jp

あらまし　GPS はいまや社会インフラともいえるほど広く利用されており，交通システムにおける利用も進められている．ただし，GPS は人工衛星からの電波を使用するので，他システムからの電波干渉や意図的な妨害により利用不能となることがあることに注意が必要である．さらに，GPS の信号を記録・再生することによる攻撃や，GPS と同一の信号を生成することで GPS 受信機に誤った位置を出力させることも考えられている．本報告は，こうした GPS におけるセキュリティの問題について述べるとともに，現在考えられている対策を紹介する．

キーワード　GPS，セキュリティ，スプーフィング

Security of GPS: Vulnerability and Countermeasures

Takeyasu SAKAI†

† Electronic Navigation Research Institute, National Institute of Maritime, Port and Aviation Technology
7-42-23 Jindaiji-Higashi, Chofu-Shi, Tokyo 182-0012 Japan
E-mail: †sakai@mpat.go.jp

Abstract　GPS is widely used in our daily lives including applications to public transportation systems. It should be noted that GPS is somehow vulnerable against radio interference and intentional jamming because it is based on radiosignals transmitted from the satellite orbit. Furthermore, we should be aware that attacking by recording and playing back GPS signals and spoofing a GPS receiver by generate fake GPS signals are technically possible. In this report, the author introduces GPS security issues and countermeasures proposed up to now.

Keywords　GPS, security, spoofing

1. はじめに

衛星航法システムの一つである GPS（Global Positioning System：全地球測位システム）は，その名の通り地球上のどこでも自分の現在位置を知るためのシステムである．もともとは米軍が開発した軍用システムであるが，一部の機能については民生用途に開放されており，幅広いユーザを得ているのは周知のとおりである．代表例はカーナビゲーションと言えるが，船舶や航空機の航法にも利用されており，最近は多くの携帯電話にも内蔵されている．

GPS の基本的な原理は，GPS 衛星が送信している無線信号を利用して，GPS 受信機が衛星までの距離を測ることによる．人工衛星が送信している電波を使用するので，上空の電波を受信できない環境では機能しない．例えば，地下やトンネル内，水中，深い谷間，ビル街といった環境では，GPS を利用できない．また，他システムからの電波干渉や意図的な妨害により利用不能となることがある．

ほかにも，GPS の信号を記録・再生することによる攻撃や，GPS と同一の信号を生成することで GPS 受信機に誤った位置を出力させることも考えられている．本解説は，こうした GPS におけるセキュリティの問題について述べるとともに，現在考えられている対策を紹介する．

2. GPS の概要

GPS では，人工衛星（GPS 衛星）からの電波を受信することで「GPS 受信機の現在位置」（経緯度と，場合によっては標高）を知ることができる[1]．このために、図 1 のように高度約 2 万 km の軌道上を 30 機程度（時期によって異なる）の GPS 衛星が周回しており，地表面に向けて常時 GPS 信号を送信している．なお，GPS は米国のシステムであるが，他にも表 1 のような衛星航法システムが運用され，あるいは構築されつつある．我が国は準天頂衛星システム（QZSS：Quasi-Zenith Satellite System）の構築を目指しているところである．

GPS 受信機は，上空の GPS 衛星が送信している GPS

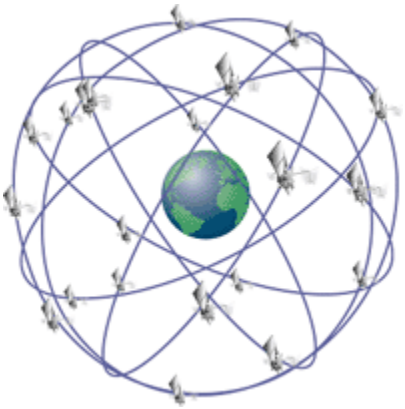


図 1 GPS 衛星の軌道（米国連邦航空局 HP より）

信号をすべて受信して，それらとの間の距離を測定する．ただし，ビル等の陰になっている衛星からの信号は受信できないから，信号を受信できる衛星の数は限られる場合がある．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できれば，GPS 受信機は自分の位置を計算できる．GPS 受信機自体の性能や周辺環境に大きく左右されるが，条件がよければ数 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．

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から，先に述べたとおりトンネルや地下街では 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．

GPS があると自分の位置を知られてしまうとの誤解が多いが，GPS はあくまでも「GPS 受信機が」「現在位置を」求めるものである．このために必要なのは GPS 衛星が送信している信号を受信することだけであって，GPS で位置を求めるために何らかの信号を送信する必要はない．すなわち GPS による位置の測定はパッシブ方式であり，それだけでは GPS 受信機の外部に何らの位置情報も伝達することはない．得られた位置情報を外部に送信するかどうかは，GPS により位置を知ることとは別の問題である．

また，GPS で得られるのは現在位置の情報だけであり，目的地にどのように向かうかについては GPS は関係ない．カーナビゲーションなら別途地図情報と照合し，ルート検索を行う必要があるが，これらは GPS 自体の機能ではない．

3. GPS の脆弱性

それでは，セキュリティ上の観点から GPS の脆弱性を検討する．対象とする事象は，自然現象以外の外部要因により，GPS 受信機が自己の位置を計算できなくなるか，計算されて得られた位置情報が（測位精度の程度を超えて）不正確となることとし，GPS 自体や利用者のエラーは含めない．GPS の脆弱性は，意図しない原因による場合と，意図（悪意）のある場合に分けて考えることができる[2][3].

3.1. 意図しない原因によるもの

2007 年 1 月，米国サンディエゴ市一帯で GPS が突然利用できなくなった．原因調査の結果，海軍船舶の通信機に不具合があり，GPS が使用している周波数帯域（1.6GHz 帯）に不要な電波を放射していたことが判明した[3]．原因はこの通信機の不具合であるが，問題はこの程度のことで広範囲に GPS を使用できなくなってしまった事実といえる．この事例では，実際に医療機関の緊急呼出しサービスに影響があったと報告されている．

GPS 衛星が送信している電波の電力は，実は 100 ワットの電球と同じ程度である．2 万 km 彼方にある 1 個の電球であるから，GPS 受信機に入ってくる GPS 信号はたいへん微弱であり，何らかの原因で近接する周波数に余計な電波が発射されると，付近の GPS 受信機はすべて使えなくなってしまう．

このような意図しない電波による影響は，干渉（interference）と呼ばれる．数年前にドイツの空港でやはり GPS が異常な位置を示す事例が報告されており，この原因は航空機格納庫に取り付けられていた GPS リピータによる電波が漏れていることであった．リピータというのは，屋内でも GPS を利用できるようにするため，屋外のアンテナで受信した GPS 信号を屋内に再送信するものである（図 2）．リピータによる信号を受信した GPS 受信機は，すべてリピータの受信アンテナの位置を示すこととなる．電波は目に見えないため，こうした事象が起きていても当事者にはわからない場合があり，原因調査には専用の機材と多くの手間がかかる．

3.2. 意図的な妨害

次に、何らかの意図をもって GPS を利用できなくする場合が考えられる．

2010 年頃から現在にかけて，韓国のソウル周辺で航空機が GPS を使用できなくなる事例がたびたび報告されている[4]．影響範囲は次第に拡大してきており，北朝鮮による妨害活動だと言われている．

米国では，しばらく前まで PPD（Personal Privacy Device）と称して GPS ジャマーが市販されていた（図 3）。これは GPS が使用している周波数帯で意図的な妨

図 2 GPS リピータの製品例
（測位衛星技術（株） GPSRKL12G）

図 3 市販されていた PPD の例

害波を発するものである[5][6]. たとえば，運送業では運行管理に GPS が使われることがあるが，これを嫌う運転手が自車の GPS を機能しないようにするのである（このため，安価な GPS ジャマーはシガレットソケットに挿し込むタイプが多い）. 前述のとおり GPS の電波は微弱であり，妨害（jamming）するのは簡単といえる. 航空機が GPS を使用する場合の危険性などを考慮して，現在はこのような機器は米国でも違法となっている.

妨害波が強いほど広い範囲の GPS 受信機を妨害できるが，一方で送信源を特定することは容易になる. 発見されないためには，なるべく微弱な電波を使用するのが有効である. 電波の形式によっても GPS 受信機に対する影響は異なってくるが，もっとも効率的に GPS 受信機を誤動作させることができるのは，実は GPS 信号そのものである. 単純な形式の電波よりも，本物の GPS 信号を使えば微弱な電波でも効果的に GPS を妨害できるのである. 先のリピータの例もある通り，これは技術的にさほど難しいことではない. GPS 信号をそのまま，あるいは加工して再送信することによる妨害を，ミーコニング（meaconing）という.

最近は携帯通信機器の開発向けに RF レコーダが市販されている. これは無線信号を直接受信・記録し，さらに再生することができる機材であるから，過去の（他の場所の）GPS 信号をプレイバックできる. 送信用のアンテナを付ければ，ただちにミーコニングデバイスとして利用できる.

プレイバック型のミーコニングの対策としては GPS 受信機が内蔵している時計の時刻と GPS 信号を比較・照合することが考えられるが，こうした対応の有無は GPS 受信機によって異なり，統一された規格は存在しない. また，プレイバック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.

3.3. 欺瞞信号

いま一つの妨害はスプーフィング（spoofing）攻撃であり，偽の GPS 信号を作り出して，GPS 受信機を欺くことを指す[7].

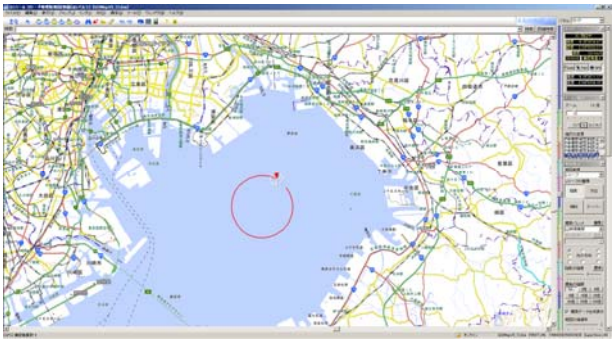
GPS 衛星が送信している民生用信号の仕様については IS-GPS という文書として公開されている（最新版は IS-GPS-200 Rev. H）[8]. その内容は GPS 受信機を製作するために必要な情報であり，すべての GPS 受信機は IS-GPS に記載されている情報にもとづいてつくられている. 民生用信号を使う限り GPS 受信機は誰でも製作できるが，その代わり GPS 信号の内容は秘密にされていない. 市販の GPS 受信機が内部で実行している処理については，特に位置の計算方法については GPS を使用する以上は既知である[9].

GPS 信号に似た信号を作り出すことは技術的に可能で，たとえば GPS 受信機メーカーにおける試験用途などのために GPS シミュレータと呼ばれる製品も存在する. 図 4 は，安価なソフトウェア無線機デバイスを使用して実際に GPS 受信機を欺いた例である. (a)は東京湾内を円状に走行させた例，(b)は仙台空港周辺における実験機航跡を再現した例である. これらは 1 分間程度の間隔で連続して実行したのであるが，受信機出力は東京湾から仙台空港にただちに移動し，何らのエラーを発することもなかった. 図 5 はこの例に使用したソフトウェア無線デバイスである.

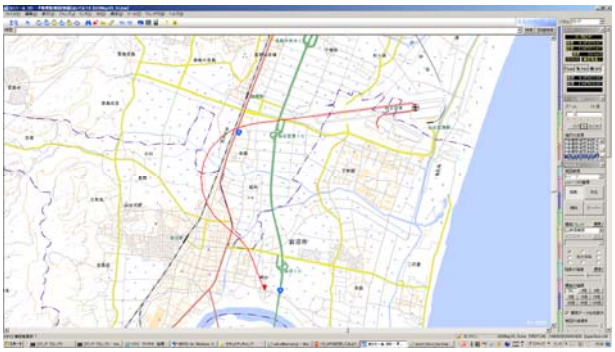
広い範囲にわたるスプーフィングは原理的に難しいが，攻撃対象を絞ればスプーフィングは可能といえる. 無人機に対するスプーフィング実験も行われおり[10][11]，スプーフィングにより船舶を誤った進路に誘導したとの実験結果も報告されている[12][13].

3.4. 位置情報の偽装

以上は GPS 信号に対する干渉あるいは妨害であったが，GPS 受信機の出力に対して意図的な操作を加え



(a) 東京湾を円状に走行させた例



(b) 実験機航跡を再現した例

図 4 スプーフィングの例

る手法も知られている．GPS 受信機が出力する位置情報は標準フォーマット（NMEA-0183 等）によることが多く，インターフェースもシリアル通信あるいはイーサネットによるものが普通であるから，物理的な偽装は可能である．

最近では，ソフトウェアによる偽装も一般に知られるようになった[14]．例えば，位置情報ゲーム「ポケモン Go」では，スマートフォン内部の API（application programming interface）を操作することで現在位置を偽装することが行われ，ゲーム運営者側が対策に乗り出している状況である．

もともと，GPS 情報を使用するアプリケーションの開発者向けに位置情報を操作するソフトウェアも存在することから，このようなことは比較的容易に可能である．特に高価なハードウェアを必要とするわけでもないから，位置情報を使用するアプリケーションの運用には注意が必要である．

4. 対策

以上に述べた GPS の脆弱性については，さまざまな対策が検討されている．干渉やジャミングについては，GPS を使用できないことが利用者にもわかるため深刻な影響はなく，必要な規制を行うことと送信源を探索する仕組みを整備すること，利用者にとっては GPS 以外の位置測定手段をもつことが対策となる．

図 5 ソフトウェア無線デバイスの例
（nuand 製 bladeRF）

問題はミーコニング及びスプーフィング，位置情報の偽装であって，これらは実行されていることが利用者にはわからず，深刻な被害を生じる可能性がある．これらの対策として考えられている手法を以下に述べる[11][15]．

4.1. 測位信号の暗号化

スプーフィング対策の一つとして，測位衛星が送信する測位信号の暗号化が考えられている[16]．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，欺瞞信号の生成を阻止しようとするものである．すでに仕様が公開されている GPS 信号に対してこのような対策を採用することはできないが，今後サービスを開始する衛星航法システムでは採用が検討されている．

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されており，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仕組みである．

ただし，復号した結果として得られる情報の形式が既知であり，かつ情報量が多くないこと，また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，暗号としての強度を保つことは難しいものと思われる[17]．測位信号の暗号化はスプーフィング対策であって，ミーコニングに対しては効果はない．

4.2. アレイアンテナ

ミーコニングやスプーフィングの特徴として，攻撃者は地上付近から送信してくることがあげられる．このため，受信アンテナに指向性をもたせて，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れば，これらの対策となる．パラボラアン

テナのような物理的に指向性のあるアンテナを用いると装置が大型になるため，複数のアンテナを用いて信号処理により指向性をもたせるアレイアンテナによる方式が主に検討されている[18][19].

このような指向性アンテナの使用は，反射波により距離測定誤差を生じるマルチパスの対策にもなる．3次元的な指向性を実現するためには最低で3式のアンテナを配置する必要がある．アレイアンテナ自体の指向方向を一定に保つ必要があることから，携帯機器での採用は難しいものと思われる．

4.3. センサフュージョン

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.

さまざまなセンサが考えられるが，たとえば車両の場合は車速センサ（回転計）を手軽に利用でき，カーナビゲーションでは標準的に使用されている．また，加速度及び角速度を測定するIMU（inertia measurement unit）センサは小型化及びチップ化が進められており，GPS受信機との相性が良いことから有望視されている[19][20]. 気圧高度計により高度情報を得て，標高データベースと照合することも可能である．最近では，CASC（chip scale atomic clock）と呼ばれる超小型原子時計が実現されており，時間差を正確に測定することで欺瞞信号を検出する試みがある[21].

こうした追加センサを用いる方式はセンサフュージョンと総称される．GPS信号の欺瞞対策としては効果的であるが，当然ながら追加のハードウェアを要する．また，絶対的な物理量を測定するセンサを使用しない限り，すなわち加速度や時間差の測定では，GPS受信機のスタートアップ時に行われるキャリブレーションに弱点があることが指摘されている.

なお，航空分野においては，GPS以外のバックアップ航法手段を確保する必要性が認識されており，APNT（alternative position, navigation, and timing）と総称されて検討が進められている．既存の無線航法施設を利用するほか，地磁気による航法なども検討されている[22].

4.4. 受信機ネットワーク

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．従って，特定の地点のGPS受信機に対してミーコニングやスプーフィ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.

こうした性質を利用して,多数のGPS受信機によるネットワークを用いるアイディアが提案されている[23]．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.

4.5. 干渉･妨害信号の検出･排除

無線信号の送信は各国の電波法制により規制されているのが一般的であり，GPSに対する干渉・妨害信号についてはこうした規制にもとづいて排除することができる．前述のとおり，以前の米国ではPPDを容易に入手できたが，GPSに対する影響に鑑みて現在は違法とされており，すでに逮捕例もある．日本においては，微弱電波でない限り無線信号を送信するには免許が必要である.

一方で，特に航空分野においては安全面から空港周辺を対象としたGPS信号のモニタリングが必要とされている.これは,GPSのユーザ（この場合は航空機）とはまた別の第三者（同じく航空局）がGPS信号の状況をモニタし，必要に応じて航空管制官等を含む関係者に情報提供をすることで，規制のみによらない安全確保を図るものである[24]．一部の国においては，さらに送信源の特定まで行うシステムも実用されている.

5. 背景：利用環境の変化

GPSに脆弱性があることは当初から指摘されていたが，その議論の中心は干渉あるいはジャミングであった2)．最近は，それらにミーコニングやスプーフィングを加えて議論されるのが普通になってきている.

この背景には，近年における位置情報の利用形態の変化がある[14].すなわち,トラックドライバーがPPDを使用するように，GPSにより自己の現在位置を監視される利用者が現れている．また，渋滞緩和のための交通規制や道路課金にGPSを使用することも一部の発展途上国で考えられている．すなわち，従前はGPS受信機を備える利用者自身がGPSによる位置情報を必要としていたのであるが，そうではない利用形態が現れてきている.

このような利用形態では，スプーフィングや位置情報の偽装に動機があることに注意しなければならない.位置情報ゲーム「ポケモンGo」で位置偽装が広く行われたのは，技術的に難しくないことも理由の一つであるが，まず第一に偽装する動機があることに注意を払うべきである．利用者自身が位置情報を必要としている従前の利用形態では，技術的に可能であったとしても，動機がなかったのである.

また，GPSの利用が拡大した結果，位置情報の取得にGPSが利用されていることが周知となっていることもリスク要因として指摘しておきたい．すなわち，

ミーコニングやスプーフィングにより，GPS を利用している移動体の進路をそれと知られることなく変更し，これを攻撃あるいは捕獲することが可能となるのである．ドローンや船舶に対するスプーフィング実験例が報告されているが，ドローンを含む移動体航法のリスクとして認識すべきである[11]．技術の進歩により，ミーコニングやスプーフィングに必要なハードウェアが比較的安価かつ容易に入手できる環境となっていることも忘れてはならない．

GPS の脆弱性については，こうした利用形態の変化，言い換えれば脆弱性を突く動機をよく認識したうえで，適切な技術的対策を検討する必要があろう．

6. むすび

いまや社会インフラとなった GPS の利用範囲は拡大の一途といえる．位置情報が関連する分野においては当然のことながら，一見関係なさそうな施設や機材でも目立たずに利用されている場合もあり，たとえば通信回線や金融機関の時刻同期といった例がある．利用範囲の拡大により利用者自身に位置情報を偽装する動機が生じている一方，無線通信デバイスの一般化により比較的安価かつ容易に GPS 信号を生成できる環境となっている点に注意が必要である．こうした背景から最近は GPS のセキュリティが問題視されており，妨害や欺瞞の対策を進める必要がある．

文　献

[1] 坂井丈泰：GPS 技術入門，東京電機大学出版局，Feb. 2003.

[2] John A. Volpe National Transportation Systems Center: Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, Aug. 2001.

[3] 水野勝成：測位衛星への干渉・妨害，安全対策，GPS/GNSS シンポジウムテキスト，pp. 248-251，Oct. 2017.

[4] D.W. Lim: Results of an Interference Detection and Localization System Operation in an Airport, Proc. ION International Technical Meeting, pp. 693-704, Feb. 2017.

[5] S. Pullen and G. X. Gao: GNSS Jamming in the Name of Privacy: Potential Threat to GPS Aviation, Inside GNSS, vol.7, no.2, pp. 34-43, March/April 2012.

[6] 福島荘之介，齊藤真二：PPD（個人用保護デバイス）の地上型衛星航法補強システムへの影響，測位航法学会論文誌，vol.6，no.1，pp. 1-6，Feb. 2015.

[7] T.E. Humphreys, P.M. Kintner, Jr., M.L. Psiaki, B.M. Ledvina, and B.W. O'Hanlon: Assessing the Spoofing Threat, GPS World, 20, 1, pp. 28-38, Jan. 2009.

[8] 米国国防総省：Navstar GPS Space Segment/ Navigation User Interfaces，IS-GPS-200H，Sept. 2013.

[9] 坂井丈泰：GPS のための実用プログラミング，東京電機大学出版局，Jan. 2007.

[10] D.P. Shepard, J.A. Bhatti, and T.E. Humphreys: Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle, GPS World, vol.23, no.8, pp. 30-33, Aug. 2012.

[11] K. Wesson and T. Humphreys: Better Security Measures Are Needed Before Drones Roam the U.S. Airspace, Scientific American, Nov. 2013.

[12] A. Cameron: Spoofer and Detector: Battle of the Titans at Sea, GPS World, Aug. 2014.

[13] J. Bhatti and T.E. Humphreys: Hostile Control of Ships via False GPS Signals: Demonstration and Detection, Journal of The Institute of Navigation, vol.64, no.1, pp. 51-66, Spring 2017.

[14] J. Curran, D. Borio, G. Buesnel, and O. Pozzobon: Cybersecurity in Localization, Coordinates, vol.13, no.1, pp. 8-13, Jan. 2017.

[15] C. Gunther: A Survey of Spoofing and Counter-Measures", Journal of The Institute of Navigation, vol.61, no.3, pp. 159-177, Fall 2014.

[16] P. Enge and T. Walter: Digital Message Authentication for SBAS (and APNT), Proc. ION GNSS+ 2014, pp. 1328-1336, Sept. 2014.

[17] T. Humphreys: Limitations of Signal-side GNSS Signal Authentication, Proc. ION GNSS+ 2014, pp. 1351-1363, Sept. 2014.

[18] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz: Direction-of-Arrival Assisted Sequential Spoofing Detection and Mitigation, Proc. ION International Technical Meeting, pp. 181-192, Feb. 2016.

[19] Y. Liu, Q. Fu, S. Li, and X. Xiao: The Effect of IMU Accuracy on Dual-antenna GNSS Spoofing Detection, Proc. ION International Technical Meeting, pp. 169-180, Feb. 2016.

[20] S. Lo: GNSS Spoof Detector for Aviation (and Other Transport Applications) using Low Cost Accelerometers, Proc. ION Pacific PNT Conference, May 2017.

[21] T. Krawinkel and S. Schon: Getting There More Safely: Better GNSS Navigation and Spoofing Detection with Chip-scale Atomic Clocks, GPS World, vol.27, no.10, pp. 50-55, Oct. 2016.

[22] A. Canciani and J. Raquet: Magnetic Anomaly Navigtation Accuracy with Respect to Map Quality and Altitude, Proc. ION International Technical Meeting, pp. 110-116, Feb. 2016.

[23] Y. Yang, H. Li, and M. Lu: Multi-user Cooperation Based GNSS Spoofing Detection Method, Proc. ION International Technical Meeting, pp. 160-168, Feb. 2016.

[24] 麻生貴広：航空機の航法における GNSS モニタリングの取組み，GPS/GNSS シンポジウムテキスト，pp. 252-258，Oct. 2017.