

協力:



Smart
Mobility
Living Lab
London

業界の見解

GPS スプーフィング: 自動車産業のリスク

ADAS (自動運転支援システム) および自動運転システムへの脅威の高まりに関する専門家の見解



FocalPoint 寄稿者: Ross van der Merwe 博士、GNSS エンジニア

J. Rossouw van der Merwe 博士は、2016 年に南アフリカのプレトリアで工学の修士号を取得しました。その後すぐにドイツに移り、フラウンホーファー IIS の研究員として働きながら、ドイツのエアランゲンにあるフリードリヒ アレクサンダー大学で GNSS スプーフィング検出と GNSS レジリエンスの博士号を取得しました。2022 年以來、英国、Focal Point Positioning の GNSS エンジニアとして従事しながら、現代の GNSS の課題解決に取り組んでいます。



自動車業界を揺るがす 新たな脅威: GPS スプー フィング

GPS スプーフィングについては、映画で見覚えがあるかと思います。しかし、スプーフィングは自動運転を現実のものとするために、自動車業界が対処する必要のある新たな脅威となっています。

GPS スプーフィングは、偽の衛星信号または記録された衛星信号を送信して、GPS 受信機 (技術的には GNSS 受信機と呼ばれます。詳細は下記を参照) が別の場所にあると思わせるサイバー攻撃の一種です。ほとんどの国では違法ですが、攻撃を実行するための機器やノウハウを入手することがはるかに容易になり、潜在的な攻撃者にとっての誘因が高まっています。

路上でドライバーが操縦する車両に対する直接的なリスクは低いものの、自動運転が判断する車両にとってGPS スプーフィングは、脅威となります。ナビゲーションシステムの GPS 受信機が、車がどこか別の場所にあると判断した場合、自動運転は予測できない判断を下す可能性があり、車両内の人や物、その他の道路利用者の安全が脅かされる可能性があります。



ガイドの内容: GPS スプーフィングとは何か、またそれを防ぐ方法

GPS スプーフィングがしやすくなっていますが、OEM や Tier 1 (ティア 1) サプライヤーにとって幸運なことに、GPS スプーフィングを解決するためのソリューションがこれまで以上に増えてきています。

このガイドでは、以下の手順で解決方法を説明します:

1. GPS スプーフィングの仕組みと GPS 受信機への影響
2. 自動車業界に及ぶ GPS スプーフィングのリスク
3. 基準と規制の現状
4. GPS スプーフィングのリスクを軽減する 4 つの技術戦略
5. 重要なポイントと次のステップ

このホワイトペーパーには、技術開発者から OEM、保険会社、政策立案者、標準化団体、消費者まで、さまざまな業界関係者がスプーフィングのリスクをどのように見ているかを理解するために、[Smart Mobility Living Lab \(SMLL\)](#) と共同で実施した調査から得られた知見が含まれています。

GPS? それとも GNSS?

このガイドでは、より専門的な用語である GNSS (全地球航法衛星システム) ではなく、GPS について話していることに気付かれると思います。それは、GNSS システムで最も馴染み深いシステムが GPS だからです。しかし、現在、衛星ナビゲーションと正確なタイミングサービスを提供する GNSS システムは、GPS、ガリレオ、GLONASS、BeiDou の 4 つです。最近の受信機のほとんどは、これらのシステムのうち少なくとも 2 つの信号を使用しますが、3 つまたは 4 つすべてを使用する受信機もあります。スプーフィングは、これらの衛星群のいずれかまたはすべてを使用している受信機に影響を及ぼす可能性があります。



GPS スプーフィング の仕組み

GPS スプーフィングは、GPS 受信機を標的とする電子妨害技術の一種です。攻撃者は送信機を使用して、実際の GPS 信号を模倣した無線信号を空中に流します。これらの偽の信号は、実際には実際の GPS 信号を記録したものである場合があります。これは「ミーコニング」と呼ばれるスプーフィング攻撃の一種です。

かつては、機器が高価で、GPS 信号と受信機のアーキテクチャに関する専門知識が必要だったため、スプーフィングデバイスの構築は非常に困難でした。しかし、ソフトウェア定義無線 (SDR)、オープンソースソフトウェア、およびスプーフィング方法に関するオンライン情報にアクセスできるようになったため、スプーフィングは次第に容易になってきました。

転機は 2016 年に、拡張現実スマートフォンゲーム「ポケモン GO」の発売とともに訪れました。ポケモンを捕まえるためには実際の場所に行く必要がありましたが、携帯電話の位置を偽装できれば家を出ることなくレア ポケモンを捕まえることができることに気付いた人もいました。ほとんどのプレイヤーは携帯電話の位置を偽装するソフトウェアを使用しましたが、少数ながら、自家製の無線機を使用するプレイヤーや、偽装に精通したゲーマー世代が生まれました。

妨害 (ジャミング) とスプーフィングの違いは？

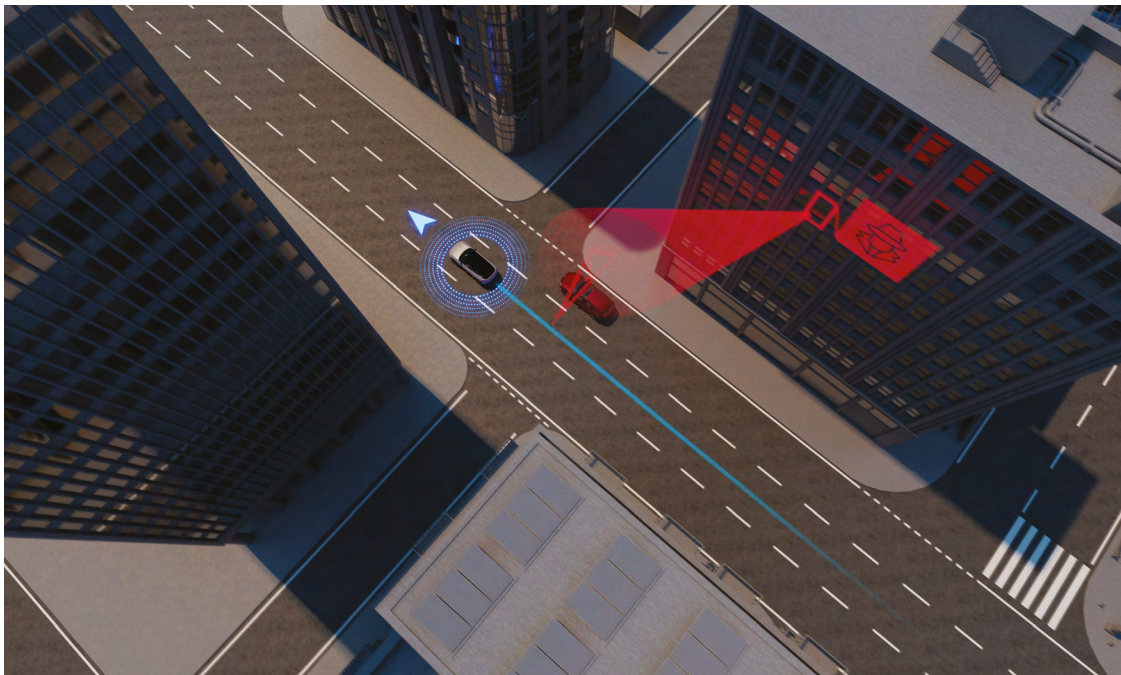
GPS 受信機に対する電子攻撃には、ジャミングとスプーフィングの 2 種類があります。ジャミングでは、GPS 信号をかき消す電磁ノイズを放送するデバイスが使用されます。受信機は微弱な GPS 信号を識別できなくなるため、位置を計算できなくなります。スプーフィングでは、スプーフィングデバイスが偽の座標を含む人工信号を送信するので、受信機が (多くの場合、非常に) 不正確な自己位置を計算することになります。



保護されていない GPS 受信機にスプーフィングが及ぼす影響

スプーフィングが効果的なのは、地上のスプーフィングユニットから送信される信号が実際の GPS 信号よりもはるかに強力であるためです。実際の GPS 信号は、受信機に到達するために、宇宙天気と地球の大気にバッファーされながら、約 20,500 マイル (32,991 km) 移動する必要があります。

本物の信号と偽の信号を区別できない保護されていない受信機は、実際の信号ではなくスプーフィング信号に簡単にロックオンしてしまいます。これは、受信機の電源を入れたばかりの場合や、建物やトンネルなどに囲まれた、GPS がブロックされる場所から出てきたばかりの場合に特に当てはまります。



過去数年間に実際に起きた事件は、スマートフォン、船舶、車両に搭載された保護されていない GPS 受信機がスプーフィング攻撃の影響を受けた場合に、何が起こるかを示しています。

- **2016 年 モスクワ:** [CNN](#) やその他のメディアは、モスクワ中心部で人々のスマートフォンが奇妙な動作をしたと報じました。地図アプリは、携帯電話の実際の位置ではなく、車で 45 分離れた ヴヌーコヴォ空港の位置を表示しました。
- **2017 年 黒海:** [Maritime Executive](#) 誌は、黒海の約 20 隻の船で航行システムが断続的な障害を経験したと報告しました。障害発生中、すべての船舶のシステムは同じ (内陸の) 場所、つまり海岸近くの空港に居ると表示しました。



- **2019 年 上海:** [Inside GNSS](#) 誌は、上海港の海運に影響を与える新しいタイプのスプーフィング攻撃について報告しました。船舶の位置を送信するために使用される自動識別システム (AIS) は、船舶が同じ場所を堂々巡りして航行していると示しましたが、実際の位置は影響を受けませんでした。
- **2019 年 ジュネーブ:** [Jalopnik](#) ウェブサイトは、ジュネーブモーターショーのいくつかの車両が展示場でスプーフィングを受けたと報告しました。ナビゲーションシステムは、車が 2036 年のイギリス、バッキンガムシャーにあるかのように誤表示しました。発生源は、出展者のブースで使用されていた GPS 信号シミュレーターが漏洩したためであると考えられています。

スプーフィング: 自動運転車のリスク

「この手法は、ドライバーに深刻な問題を引き起こす可能性があります。また、将来、自動運転車は、このような攻撃に対して非常に脆弱になり、意図しない場所に運転されてしまう可能性があります。」

— Jason Torchinsky 氏、[Jalopnik](#) 誌、2019 年 3 月

- **2024 年 イスラエル:** [BBC](#) は、イスラエルとガザでの紛争による GPS の中断が民間人のスマートフォンアプリに影響を与えていたと報告しています。BBC のプロデューサーは、エルサレムにいるのに、携帯電話は自分がカイロにいると表示しており、これはスプーフィング攻撃を示唆するものだと言いました。



現実世界のスプーフィング攻撃から学ぶ重要な教訓

これらのメディア報道は、保護されていないGPS受信機がスプーフィングに対してどのように動作するか、そして自動車業界に及ぼす潜在的な影響について、多くのことを教えてください。OEM および Tier 1 サプライヤーにとって、特に注目すべき点は次のとおりです。

- **保護されていない受信機は誤った位置を計算する:** 受信機は、攻撃の影響を受けるとすぐに誤った位置の計算を開始します。ジュネーブ モーターショーでは、出展者が車両のナビゲーションシステムをリセットしようとしても、システムは再び誤った信号にロックオンしました。これはおそらく、モーターショーが屋内で行われ、実際の GPS 信号が通常届かないためだと考えられます。
- **多くのデバイスは何が起こったかを認識していない:** これらの攻撃の影響を受けた受信機はいずれも、位置が突然変化した際に警報を発しなかったようです。スマートフォンから船舶、車両に至るまで、多くのナビゲーションシステムは新しい座標をそのまま受け入れ、誤った位置を表示してしまっているようです。
- **受信機は意図したターゲットではない可能性がある:** 受信機がスプーフィング攻撃の対象でなくても影響を受けます。たとえば、モスクワと黒海での事件は、**軍用グレードの対ドローン装置**によって引き起こされたという強力な証拠があります。大きな手がかりは偽装された位置情報にあります。影響を受けたスマートフォンと船舶のナビゲーションシステムは空港の位置を報告していました。多くのドローンにはジオフェンスが組み込まれており、空港に近づくとき着陸したり帰還したりします。これらの攻撃の背後にはおそらくドローン対策の意図があったと思われますが、いずれの場合も送信機が非常に強力であったため、スマートフォンや、引いては海運にも影響を及ぼしました。

知っておくと便利

GPS スプーフィング攻撃の標的になっていなくても、被害を受ける可能性があります。単に、たまたま「悪い場所」に「悪いタイミング」で居合わせただけで被害を受けてしまいます。

- **紛争地域ではリスクが高い:** 中東などからの最近の報告によると、GPS スプーフィングは現在、GPS ジャミングに加えて軍事戦術としても使用されていることが示唆されています。紛争地域内またはその付近で使用される保護されていない受信機は、特にスプーフィングの危険にさらされる可能性があります。



重要なポイント：
GPS スプーフィングは保護されて
いない受信機にとって現実的な脅
威であり、スプーフィング攻撃が容
易になっており、世界中の多くの場
所で攻撃が報告されています





自動車業界に及ぶ GPS スプーフィングの リスク

スプーフィングは現時点ではリスクの低い脅威であるものの、車両の自律性が向上するにつれてリスクが増加するというのが、自動車業界の現在の認識です。バリューチェーン全体の関係者が SMLL に当社アンケートで語った内容は次のとおりです：

- **OEMとサプライチェーン:** 自動車メーカーとその Tier 1 サプライヤーは、スプーフィングがリスクであることを認識はしていましたが、スプーフィングを行う強い動機が現れない限り、現在の脅威の規模については保守的な見解を取っていました。車両の自動化が進むにつれて、将来的にはリスクが高まると予想しています。偽の信号を検出し、車両が安全に走行を継続できない場合にリスク最小化制御 (MRM) を実行する機能を含む、スプーフィング防止機能がマルチセンサー測位システムに組み込まれることが強く期待されていました。
- **保険会社:** 話を伺った保険会社は、保険料の引き下げや事故の責任の隠蔽を目的として、テレマティクス システムを「操作」するためにスプーフィングが使用されることを懸念していました。
- **技術開発者:** ナビゲーション システムとサービスの開発を担当するエンジニアは、特に自動運転車や自律走行車に対するスプーフィングの脅威を認識していました。車両の自律性が高まるにつれてリスクは増大するばかりであると指摘しました。また、スプーフィングに対して脆弱なセンサーは GPS だけではなく、カメラ、LiDAR、レーダーもすべて騙される可能性があるかと指摘しました。
- **政府機関:** 私たちが話を聞いた政策立案者たちは、スプーフィングがもたらすリスクをあまり認識していませんでした。主な懸念は GPS ジャミングであり、特に車両盗難の補助として使用された場合に関するジャミングでした。道路車両に対する GPS ハッキングの実際の事例は知りませんでしたが、車両の自律性が高まるにつれてリスクになる可能性があることは認めていました。道路車両におけるスプーフィングの脆弱性と緩和策を評価するための、制御されたテスト環境の必要性が提起されました。
- **エンジニアリングコンサルタント企業および標準化団体:** これらの団体は、自動運転支援システム (ADAS) や自動運転車に対するその他のリスクとともに、スプーフィングのリスクを認識していました。スプーフィングに関する規格、テスト施設、テストプログラムの必要性を指摘しました。



消費者の考えは?これとは別に、米国と英国の成人 3,000 人を対象に YouGov と共同で実施した調査で、GPS スプーフィングについての考えを消費者に尋ねました。主な調査結果は次のとおりです:

- 62% がGPSスプーフィングのリスクに気づいていませんでした
- このコンセプトを紹介したところ、81% が自動運転システムのリスクについてある程度懸念していると回答しました
- 84% が、最も懸念することは事故のリスク、または他の道路利用者や歩行者への危害のリスクであると回答しました
- 45% は、車両のスプーフィング対策機能の有無が、車両購入の選択に影響すると回答しています

スプーフィング干渉の潜在的な発生源

スプーフィング攻撃を受けるリスクは今日では低いように思われるかもしれませんが、個人的な利益のためであれ、上司の指示であれ、偽の GPS 信号を送信する用意のある人がいることを示す証拠があります。攻撃を実行する可能性のある人物や組織の種類は次のとおりです:

- **ドライバー:** ドライバーが自分の車のナビゲーションシステムをスプーフィングする動機には、たとえば、高速道路通行料金の自動支払いを避けるためなどにあります。GPS 位置をわずかに調整するだけで、車両を高速道路から小道に移動させることができ、料金徴収ソフトウェアの起動を回避できる可能性があります。

ジャミングの場合と同様に、スプーファの範囲が車両を超えて拡張し、近くの機器に影響を与え始めると、実際のリスクが発生します。例えば、2012 年には、ドライバーが GPS ジャマー (妨害装置) を使って雇用主が設置したテレマティクスシステムを無効にした事件があります。通過した場所の近くにあった、ニューアーク空港の GPS 誘導着陸システムに対して不慮により有害な干渉を引き起こしたため、\$32,000 の罰金を科せられました。

- **実験的な者:** 研究者やプロのサイバーセキュリティ研究者は、2019 年のテスラモデル 3 での実験のように、車両で GPS スプーフィング実験を行うことがよくありますが、これらはすべて制御された条件下で行われています。リスクは、好奇心旺盛、いたずら好き、または無謀な人が、交通量の多い道路や交差点でスプーファを作動させた場合に何が起こるかを調べようとする可能性があることです。実際には、投獄されるというリスクは、どれほど無法な実験者であろうかと思いとどまらせるのに十分でしょう。しかし、業界としてこのリスクを認識しておくことは依然として重要です。



車両へのサイバー攻撃が増加中

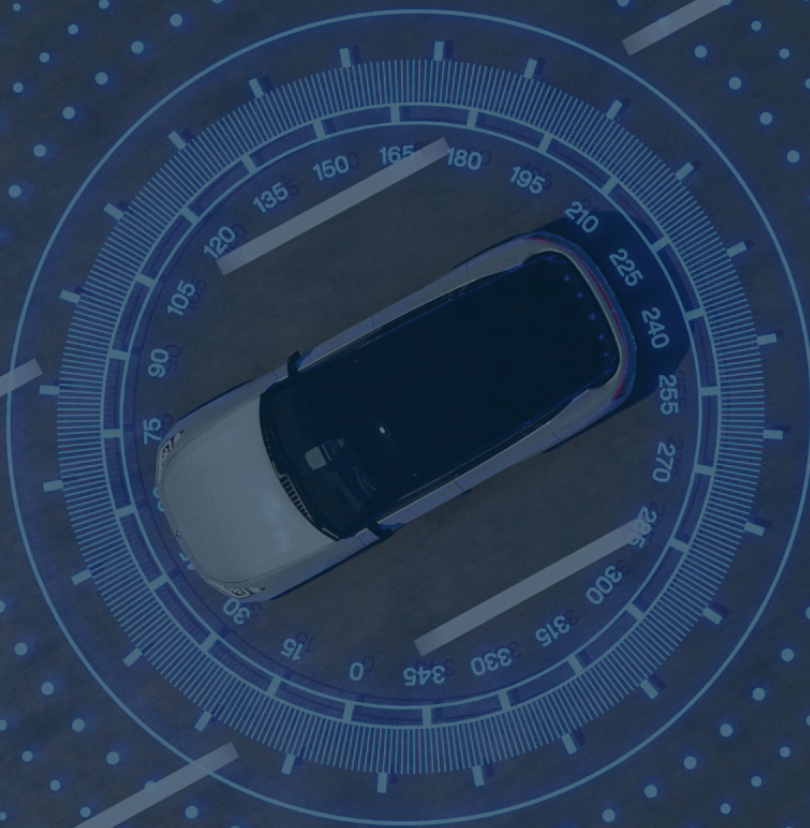
車両に対するサイバー攻撃は、2010 年～2023 年の 13 年間で 1,468 件だったのに対し、2023 年にはこの年だけでも 295 件が報告されています。

出典: [Upstream Security](#)

- **軍事作戦:** 電子戦は今や紛争地域における軍事戦術の不可欠な部分となっています。電子戦の一部としては、航法戦 (NAVWAR) があります。かつての NAVWAR 戦術は、敵の活動をジャミングするために GPS 周波数を妨害することにおおむね限られていましたが、上記のとおり、現在ではスプーフィングが蔓延しつつあります。広範囲の領域でジャミングやスプーフィングが発生すると、保護されていない GPS 受信機が電子的な集中砲火に巻き込まれる可能性があります。



重要なポイント：
業界関係者は、車両の GPS スプー
フィングのリスクが増大しているこ
と、並びに自動運転車がより脆弱に
なり、解決策が必要であることを認
識しています。





基準と規制の現状

完全自動運転の実現が近づくにつれ、標準化団体は GPS スプーフィングやその他のサイバー脅威のリスクを軽減するのに役立つテストとフレームワークの定義に取り組んでいます。標準が進化し続ける中、以下の組織に注目する価値があります：

- **ISO: [ISO SAE 21434](#)** 規格は、道路車両におけるサイバーセキュリティリスク管理の主要な国際標準規格です。ここではサイバーセキュリティのリスクを特定して対処するためのフレームワークを提供しますが、GPS スプーフィングのリスクに具体的に対処する方法は示されていません。
- **自動車技術会 (SAE):** SAE は、自動運転車のサイバーセキュリティに関する標準を開発してきました。[SAE J3061](#) 規格は一般的な車両のサイバーセキュリティに関するガイダンスを提供していますが、同様にスプーフィングについては直接取り上げていません。
- **アメリカ国立標準技術研究所 (NIST):** NIST は、サイバーセキュリティのさまざまな側面に関するガイドラインと推奨事項を提供しています。自動運転車だけに焦点を当てては 아니ませんが、GPS の整合性にとって重要な[時刻と周波数のセキュアな同期に関するガイダンス](#)は重要かもしれません。
- **米国運輸省道路交通安全局 (NHTSA):** 米国では NHTSA が自動運転車に関する規制に積極的に取り組んでいます。主に安全性に重点を置っていますが、サイバーセキュリティも重要な要素です。[NHTSA](#) のガイドラインと規制は、サイバーセキュリティ上の懸念として GPS スプーフィングに間接的に対処している可能性があります。
- **英国王立航海協会 (RIN):** RIN は、GNSS の脆弱性とリスクの評価に役立つ[リソース](#)を提供しています。同協会の測位、航行、タイミング (PNT) 諮問グループも、英国におけるレジリエント PNT の採用に関する推奨事項が記載された[ホワイトペーパー](#)の一部は、英国政府の[レジリエント PNT フレームワーク 10 項目](#)に反映されています。



重要なポイント：
GPS スプーフィングのリスクに対
処するための基準は進化しており、
自動車 OEM および Tier 1 サプラ
イヤーは動向を注視する必要があります。



GPS スプーフィングのリスクを軽減する 4 つの技術戦略

GPS スプーフィングは、スプーフィングに対して脆弱なシステムにとってのみ問題となります。そのため、特に車両の自律化が進むにつれて、PNT システムの保護は業界にとって重要な懸念事項となるはずです。スプーフィングのリスクを軽減するのに役立つ 4 つの技術戦略には、次があります：

1. マルチ GNSS、マルチ周波数チップの使用

1 つの周波数 (L1 など) で 1 つの GNSS システム (GPS など) をスプーフィングするのは比較的簡単ですが、複数の周波数 (L1 と L5 など) で複数の GNSS システム (GPS、GLONASS、ガリレオなど) からの信号をスプーフィングするのは難しくなります。したがって、マルチ GNSS、マルチ周波数チップセットを使用すると、スプーフィングに対するある程度の保護が可能になります。皮肉なことに、地域政策によっては、他国の GNSS インフラへの依存に対する懸念から、チップは 1 つの指定されたシステムのみを使用することを義務付けている国もあります。これにより、送信する必要のある偽の信号が少なくなるため、受信機がスプーフィングされやすくなります。

2. 複数の測位センサーを使用する

すべてのセンサーには脆弱性がありますが、すべてが同じように脆弱というわけではありません。LiDAR、レーダー、カメラなどの追加の測位センサーからのデータは、GPS 受信機によって計算された位置を検証するのに役立ち、さらに重要なことに、矛盾があれば警告することができます。

3. ハードウェア スプーフィング防止アンテナ

偽造された信号を本物の信号と区別する方法の 1 つは、受信機への到着角度です。本物の GPS 信号は宇宙から来るため、標高の高いところから到着する傾向がありますが、スプーフィングは通常、地上または地上近くにあるため、信号は標高の低いところから到着します。物理的なアンテナソリューションには、標高の低いところから到着したすべての信号をブロックする単純なチョークリングアンテナから、高度なデジタル信号処理アルゴリズムと適応型ビームフォーミングアンテナを組み合わせる偽装信号を識別し、アンテナのビームを偽装信号から遠ざける高度な適応型アンテナシステムまで多岐にわたります。



4. ソフトウェアによるスプーフィング防止アンテナを使用する

上で説明したタイプの物理アンテナの問題は、車両の設計とコストに大きなトレードオフが生じることです。チョークリングアンテナや適応型アンテナはかさばり、車両の空力特性に支障を来す可能性があります。適応型アンテナも非常に高価であり、そのデジタル信号処理アルゴリズムには、かなりのオンボード計算能力が必要になる場合があります。はるかに手頃な価格で設置面積の少ない代替手段は、GPS 受信機に埋め込まれた合成ソフトウェアアンテナを使用することです。この次世代テクノロジーは、アンテナで受信された信号を処理し、偽装された信号を除去して、信頼できる見通し内信号のみを残します。

規模の経済性をもたらすソフトウェアアンテナ

実際のところ、特に自動運転車向けのスプーフィング防止ソリューションには、マルチ GNSS、マルチ周波数チップセット、複数の種類の測位センサー、およびスプーフィングされた信号を除去するデジタル信号処理を備えた、アンテナソリューションの組み合わせが必要になる可能性があります。ただし、コスト、美観、オンボード計算能力は OEM にとって重要な懸念事項であるため、ソフトウェアアンテナソリューションはハードウェアアンテナよりも魅力的な選択となる可能性があります。





重要なポイント：
GPS スプーフィングのリスクを軽減
するための技術は現在存在します。
特にソフトウェアベースのアンテナ
技術は、コストと設計上の多くの障
壁を取り除いています。





自動車業界にとっての重要なポイントと次のステップ

本ホワイトペーパーで示したように、GPS スプーフィングは動的かつ進化している脅威であり、対策を講じなかった場合、ハンズフリー運転システムや自動運転車にリスクをもたらす可能性があります。

OEM と Tier 1 サプライヤーにとって、ここで取り上げた 4 つのポイントは、GPS スプーフィング対策の考え方、計画、次のステップへの指針となります。

- GPS スプーフィングは保護されていない受信機にとって現実的な脅威であり、スプーフィング攻撃が容易になっており、世界中の多くの場所で攻撃が報告されています。
- 業界関係者は、車両の GPS スプーフィングのリスクが増大していること、並びに自動運転車がより脆弱になり、解決策が必要であることを認識しています。
- GPS スプーフィングのリスクに対処するための基準は進化しており、OEM およびサプライヤーは動向を注視する必要があります。
- GPS スプーフィングのリスクを軽減するための技術は現在存在します。特にソフトウェアベースのアンテナ技術は、コストと設計上の多くの障壁を取り除いています

Supercorrelation™ で行う GPS スプーフィング対策

FocalPoint は数年前から自動車業界と協力して、GPS スプーフィングのリスクを含む、GPS の精度、信頼性、整合性の問題への取り組みを支援してきました。

その結果として生まれたのが、[Supercorrelation™](#) 技術を採用した S-GNSS Auto ソフトウェアソリューションです。Supercorrelation は、車両の軌道を計算し、その軌道に沿った [合成開口アンテナ](#) を作成することでスプーフィング信号を除外し、測位の完全性と信頼性を大幅に向上させます。

また、Supercorrelation は受信機または GPS チップセット上でソフトウェアとして動作します。そのため、自動車 OEM や Tier 1 にとっては、現在の ADAS システムと将来の完全自動運転車の両方において、GPS 受信機の統合性を大幅に向上させるための手頃な方法となります。



Supercorrelation™ 技術を搭載した S-GNSS® Auto について詳しく見る

S-GNSS® Auto に関する詳細情報、またはソフトウェアの動作デモを見るには、auto.focalpointpositioning.com をご覧ください。もしくは、ぜひお問い合わせください。



詳細に関するお問い合わせ

ハンズフリー運転をより安全かつ利用しやすくする、当社の次世代 S-GNSS Auto® ソリューションについての詳細情報を提供いたします。

contact@focalpointpositioning.com までお問い合わせください

当社は、無線受信機の精度、信頼性、セキュリティを向上させる画期的な技術を開発しています。

チップセットメーカーや OEM は当社と提携してデバイスの機能を強化し、位置情報技術を利用する何十億もの人々の生活を向上させています。

auto.focalpointpositioning.com

フォローする:

