サイバー戦入門　その８
～センサ・セキュリティ～

三村　守（防大情報工学科）

１　はじめに

情報通信技術は急速に普及し、コンピュータやインターネットの技術が生活に密接に関係するようになってきた。２０１３年度にはわが国におけるインターネットの普及率は８０％を越え、従来のパソコンに代わり、スマートフォン、タブレット、ゲーム機、音楽プレイヤー等のインターネットに接続できるＩｏＴ[1]機器の割合が増加してきた[2]。ＩｏＴとは、従来は主にパソコンが接続されたインターネットやＬＡＮ[3]に、同様の仕組みを搭載したそれ以外の機器を接続する概念等の総称である。これら機器はＩｏＴ機器と呼ばれ、スマートウォッチ等のウェアラブルデバイス、デジタル家電、子供向けの玩具、スマートカー、スマートホーム、スマートメータ等、あらゆるモノが対象となってきている。ＩｏＴ機器には、センサと呼ばれる現実の環境をモニタする機器を搭載しているものも多い。例えば、ほとんどのスマートフォンには、カメラ、マイクの他にも、位置情報を取得するためのＧＰＳ[4]センサや、磁気、加速度、ジャイロ、環境光センサ等が搭載されている。もっともスマートフォンについては、その高機能性や仕組みはもはやパソコンに近い。これらのセンサから入力された情報はデジタルデータに変換され、情報処理技術を用いて処理され、利便性の高いサービスを実現している。例えば、カメラで撮影した画像から個人の顔を識別することによって、持ち主以外の利用を防ぐ顔認証機能が実現している。あるいは、マイクから音声を入力することにより、タッチパネルを用いなくてもスマートフォンに命令を出す音声アシスタンス機能もある。さらに、これらの現実の環境とコンピュータの技術を結びつける個々の機能を組み合わせることで、より高度で複雑なサービスを実現することも可能となる。

例えば、自動車の自動運転サービスは全国各地で実証実験が進んでおり、その実現は間近であると考えられている。自動運転サービスの実現には、多くのセンサや機能が関係している。その代表的なセンサは、カメラ、レーダー及び超音波センサであり、近年ではこれにレーザー光を用いるＬｉＤＡＲ[5]も加わろうとしている。これらのセンサは、自動車に運転の指令を与えるために、人間の目や耳の

---

[1] IoT (Internet of Things) モノのインターネット

[2] 総務省(2017).「平成２９年度　情報通信白書」

[3] LAN (Local Area Network)

[4] GPS (Global Positioning System)

[5] LiDAR (Light Detection and Ranging あるいは Laser Imaging Detection and Ranging) レーザー光を用いて物体との距離を計測する技術

ような役割を果たしている。交通事故の原因は、９割以上が人為的ミスによるものだとされている[6]。よって、コンピュータ制御による自動運転サービスは、人為的ミスを局限し、交通事故の減少に寄与することが期待されている。しかしながら、２０１６年５月には米国テスラ社の自動運転車による初の交通事故が発生した。テスラ社によると、自動運転車は中央分離帯のある道路を自動運転で走行しており、前方で交差点を左折しようとした大型トレーラーに衝突した。交通事故の原因は、後方の空の光と白い色のトレーラーの側面を自動運転サービスが区別できず、ブレーキが作動しなかったためであるという。類似の事故は、無人機やあらゆるビークルの操縦においても発生し得ることが想像できる。例えば、２０１１年にはイランにおいて、米国の無人機を偽のＧＰＳ信号により着陸させたとする事例が発生している。さらに、２０１８年１月には、シリアのフメイミム空軍基地のロシア軍がイスラム国とみられるドローンの編隊の攻撃を受けたが、このうち３機の制御を奪って着陸させることに成功している[7]。自動運転サービスや自動操縦におけるセンサからの情報は、その動作に致命的な影響を与える可能性がある。今回の交通事故では、自然発生した状況に自動運転サービスが対応することができなかった。しかしながら、自然発生した状況ではなく、悪意ある者が意図的にセンサに誤動作を引き起こさせる攻撃の可能性も否定できない。

本稿では、このようなセンサに意図的に干渉して無力化する攻撃や、誤動作を引き起こさせるような攻撃について取り扱う。この問題は、センサ・セキュリティあるいは計測セキュリティと呼ばれている。以下、第２節ではセンサ・セキュリティの具体的な事例について述べる。第３節では主にＩｏＴ機器に搭載されるセンサの役割について述べ、第４節ではセンサへの攻撃を体系的に整理する。第５節ではその対策の例を示し、最後にまとめと今後の課題について述べる。

２　センサ・セキュリティの事例

センサ・セキュリティに関する具体的な事例は、これまでには主に研究分野において報告されている。

２０１３年には、心臓のペースメーカーのマイクに電磁波を照射し、健常者の心音のアナログ音声を偽装する攻撃が可能であることが報告されている[8]。ペースメーカーは、心臓の電気信号を監視することで不整脈等を感知し、要すれば電気刺激を行って鼓動のリズムを整える働きをする。そのため、健常者の心音数が誤ってペースメーカーに伝われば、不整脈等を感知することができなくなる可能性がある。従来のＩｏＴ機器への攻撃では、主にネットワーク通信やソフトウェア

[6] 米運輸省道路交通安全局(2015). "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey"
[7] Nick Waters (2018). "The Poor Man’s Air Force? Rebel Drones Attack Russia’s Airbase in Syria"
[8] Kune, D.F. et al. (2013). "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors"

のアップデートが用いられてきたが、この事例ではセンサであるマイクがアタックサーフェスとして用いられている点が目新しい。なお、医療機器に関しては、以前からセンサを用いた手法以外でも様々な攻撃が報告されている[9]。

２０１５年には飛行中のドローンに超音波を照射し、センサであるジャイロスコープに共振振動を発生させ、動作を停止させる攻撃が報告されている[10]。ジャイロスコープは物体の角度や加速度を検出するセンサである。携帯電話等の小型機器やドローンでは、振動式のジャイロスコープが用いられている。ドローンではジャイロスコープから機体の角度を検出し、姿勢を自動的に制御して安定した飛行を実現している。そのため、ジャイロスコープの動作が妨害されれば、ドローンは安定した飛行ができなくなってしまう。なお、ドローンに偽装した操作信号を受信させ、制御を奪うことによって無力化してしまう製品等もある。

２０１６年には、薬を投与する点滴のセンサにレーザー光を照射し、医療機器の誤動作を引き起こす攻撃が報告されている[11]。医療機器の中には、赤外線センサを用いて落下する水滴の数を数え、投与量を一定に制御しているものがある。これらの機器では、投与量を一定に制御するために、落下した水滴の数に応じて投与量を増減させる機能がある。ここで、赤外線センサにレーザー光を照射し、水滴の数を数えることができなくすれば、投与されていないという誤った情報が機器に伝わり、投与量を増やそうとしてしまう。患者に対する薬の投与量の増減は、生命と健康に致命的な影響を与える可能性がある。

音声アシスタンス機能を標的とし、正当な利用者に気づかれないように命令を入力する攻撃も報告されている。２０１６年には、音声認識のアルゴリズムを悪用し、音声の命令に雑音を付加して意味不明な音に変換し、何の命令かを気づかれずに入力する攻撃が報告されている[12]。この手法では、不自然な雑音が付加されるため、利用者は何らかの異変に気づく可能性が高い。２０１７年には、通常の人間には聞こえない超音波を用いて命令をマイクに入力する攻撃が報告されている[13]。この手法では、利用者は異変があったことに気づくことすら困難である。

２０１７年には、反射光を偽装したレーザー光をＬｉＤＡＲセンサに照射し、存在しない幻の目標を認識させるだけでなく、実在する目標を近くに認識させる攻撃が可能であることが報告されている[14]。ＬｉＤＡＲはレーザー光を照射し、

---

[9] IPA (2014). 「医療機器における情報セキュリティに関する調査」

[10] Son Y. et al. (2015). "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors"

[11] Park Y. et al. (2016). "This aint your dose: Sensor Spoofing Attack on Medical Infusion Pump"

[12] Nicholas Carlini et al. (2016). "Hidden Voice Commands"

[13] Guoming Zhang et al. (2017). "DolphinAttack: Inaudible Voice Commands"

[14] Shin H. et al. (2017). "Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications"

その反射光を測定することで物体の形状を感知する。そのため、センサにレーザー光を照射したり、反射光を偽装した光を照射したりすることで、誤った目標を認識させることが可能である。これにより、意図的に交通事故が引き起こされる可能性も否定できない。ＬｉＤＡＲは車の自動運転サービスに必要なセンサのひとつであるだけでなく、無人機やロボットの目としての役割も期待されており、このような脅威の影響範囲は今後ますます広がっていくものと考えられる。

２０１９年には、航空機の計器着陸装置に対してソフトウェア無線機で偽装した電波を照射し、リアルタイムで任意の侵入経路を示すことが可能であることが報告されている[15]。この攻撃により、着陸する航空機の妨害、滑走路のオーバラン、あるいは侵入経路を完全に見失う危険性等が指摘されている。

３　センサの役割

センサを搭載したＩｏＴ機器は、本体である組込システム、センサ及びアクチュエータから構成されている。センサとアクチュエータの関係を図１に示す。

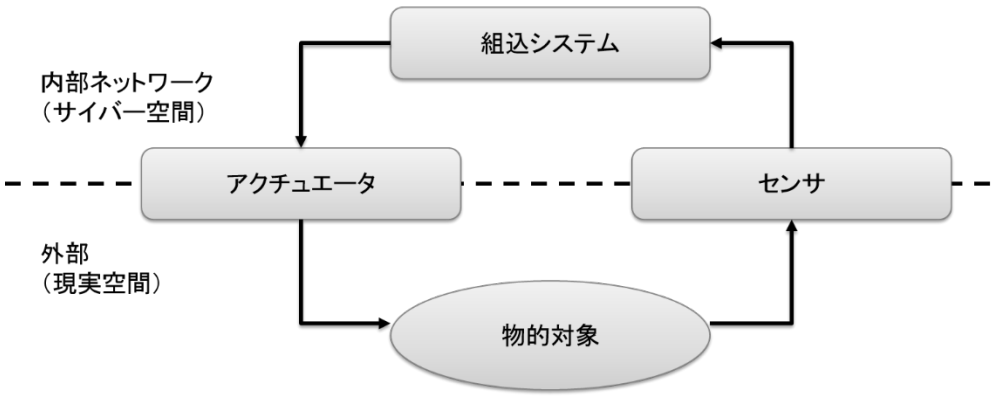

図１：センサとアクチュエータの関係

カメラ、ジャイロスコープ等のセンサは、外部の現実空間の物的対象をデジタルデータとして処理し、本体である組込システムに送信する。ここで送信されるデジタルデータは、カメラであれば画像、ジャイロスコープであれば角度や加速度となる。主なセンサとその用途を表１に示す。

表１：主なセンサとその用途

センサの種類		入力	用途
パッシブ	カメラ	画像	画像による状態の認識
	マイク、スピーカー	音声	音声による命令の認識
	ジャイロスコープ	磁気	姿勢制御
	加速度センサ	超音波	
	ＧＰＳ	信号	緯度経度把握

[15] Harshad Sathaye et al. (2019). "Wireless Attacks on Aircraft Instrument Landing Systems"

アクティブ	レーダー	電波	物体の測位（主に距離）
	超音波センサ	超音波	
	ＬｉＤＡＲ	レーザー光	
	ソーナー	音波	

センサの動作原理に着目すると、センサはパッシブ方式とアクティブ方式に分類できる。パッシブ方式のセンサは、能動的に電波等を発信せず、受動的に入力を受信するセンサである。最も基本的なパッシブ方式のセンサの例としては、カメラ、マイク等が挙げられる。カメラは撮影する画像を入力とし、画像処理技術を用いて撮影した画像を解析し、その意味を解釈して状態を把握するために用いられることが多い。例えば、自動運転車で道路上を走行するためには、画像等から道路を認識する必要がある。マイクやスピーカーの代表的な用途としては、音声によるアシスタンス機能が挙げられる。ｉＰｈｏｎｅのＳｉｒｉ、「ＯＫ Ｇｏｏｇｌｅ」のフレーズでおなじみのＡｎｄｒｏｉｄ端末、Ａｍａｚｏｎ Ｅｃｈｏ等のスマートスピーカーでは、音声のみで音楽の再生、ニュースの読み上げ、アラームのセット等の命令を実行することが可能である。スマートフォンにも搭載されているジャイロスコープや加速度センサは、磁気や超音波から物体の姿勢を把握することが可能である。これらは、無人機の姿勢制御にも用いられている。ＧＰＳについては今や説明するまでもなく、地球上のあらゆる場所において衛星からの信号を受信し、緯度経度を把握するために用いられている。

これに対してアクティブ方式のセンサは、能動的に電波等を発信し、その反射波等を入力として受信するセンサである。なお、アクティブ方式のセンサには、ソーナーのようにパッシブ方式で運用することが可能であるものもある。アクティブ方式のセンサの多くは、物体の位置を測るために用いられている。アクティブ方式のセンサに求められる特性は、物体から反射し（反射性）、同じ速度（等速性）でまっすぐ進む（直進性）ことである。これら特性をもつものとして、電波、音波、超音波、レーザー光等が用いられている。これらを物体に照射して反射波等を得ることができれば、速度×時間÷２の式から物体の距離を算出することができる。また、照射した方位から物体のおおよその方位を得ることもできる。

本体である組込システムは、センサから送信されたデジタル情報を処理し、カメラに映った物体や機体の角度から現在の姿勢を認識したりする。これらの処理は、機器の内部ネットワークであるサイバー空間において実施されている。外部である現実空間に対する干渉は、組込システムからアクチュエータに命令を送信することで実現される。

４　センサへの攻撃

これまでに示したＩｏＴ機器への攻撃を、その攻撃源を基に分類すると、内部

ネットワークからの攻撃と外部からの攻撃に分類することができる。内部ネットワークからの攻撃は、ＩｏＴ機器内部のネットワークに接続するノードを起点として論理的に実施される攻撃であり、どちらかというと伝統的なサイバー攻撃と同じような手法で実施される。外部からの攻撃は、ＩｏＴ機器の外部を起点として物理的な手段で実施される攻撃であり、これまでにあまり実施されていなかった新たなアタック・サーフェスであると言える。

（１）内部ネットワークからの攻撃

内部ネットワークからの攻撃は、攻撃者が内部ネットワークに接続するノードの制御を奪うことで実現可能となる。攻撃者は内部ネットワークに接続するノードの制御を奪うと、そのノードを起点として内部のネットワークのトラフィックを監視し、メッセージを盗聴したり、あるいは改ざんや偽のメッセージを送信したりすることが可能となる。また、これらの手法を応用した様々なサイドチャネル攻撃[16]が可能となる。これらの攻撃は、内部ネットワークというサイバー空間において実施される攻撃であるため、その手法は基本的に伝統的なサイバー攻撃と同じである。したがって、伝統的なサイバー攻撃手法の多くは、内部ネットワークからの攻撃に応用することが可能である。

攻撃者が内部ネットワークに接続するノードの制御を奪う手段としては、そのノードのＵＳＢポート、赤外線ポート、無線ネットワーク等の正当な通信手段を介してアクセスする手法が多い。また、内部ネットワークのケーブルの盗聴、不正な機器の接続等の何らかの物理的手段を用いる場合もある。

（２）外部からの攻撃

外部からの攻撃は、攻撃者が外部からセンサに対して何らかの手段で干渉することで実現可能となる。センサに干渉する手法は、対象となるセンサの種類によって異なる。パッシブ方式のセンサを攻撃するためには、こちらから単純にセンサに対して偽の画像を表示させたり、電波等を照射したりして干渉すればよい。これに対し、アクティブ方式のセンサへの攻撃はやや複雑である。アクティブの方式のセンサではセンサ自身が電波等を発信してその反射波等を利用するため、この影響を考慮してセンサに対して電波等を照射する必要がある。

主なセンサへの攻撃手法の例を表２に示す。

センサの種類		攻撃手法	影響
パッシ	カメラ	偽画像入力	無力化、状態の誤認識
	マイク、スピーカー	偽音声入力	無力化、命令の誤認識
	ジャイロスコープ	偽磁気照射	姿勢制御不能

[16] 装置内部のセンシティブな情報を取得しようとする攻撃の総称であり、暗号解読等に用いられている。

ブ	加速度センサ	偽超音波照射	
	ＧＰＳ	偽信号照射	測位不能、位置の誤認識
アクティブ	レーダー	偽電波照射	物体の測位（方位及び距離）不能、位置の誤認識
	超音波センサ	偽超音波	
	ＬｉＤＡＲ	偽レーザー光	
	ソーナー	音波	

表２：主なセンサへの攻撃手法の例

パッシブ方式のセンサに対しては、それぞれのセンサに対して偽の画像、音声、信号等が入力されるようにすることにより、センサやその機器を無力化したり、状態や命令を誤認識させたりする攻撃が考えられる。例えば、カメラに映された物体を識別する機器を考えた場合、カメラや物体に覆いをかぶせて隠してしまえば、この機器は物体を認識することができなくなってしまう。同様に、何らかの異なる物体をカメラに映るようにすれば、物体や状態を誤認識させることが可能であると考えられる。例えば、人間の顔を識別して追跡するシステムに対し、サングラス、帽子、マスク等で追跡を回避する手法が提案されている。近年では、画像認識の分野ではニューラルネットワークを用いた手法が大きな成果をあげている。これに対し、ニューラルネットワークに意図的に誤認識を起こさせるような攻撃手法も提案されている。これらの手法は、カメラをセンサとして用いたシステムを攻撃する用途に応用される可能性がある。マイクやスマートスピーカーを用いた音声アシスタンス機能に対しては、大音量の雑音により無力化することが可能であると考えられる。また、利用者の音声を録音したり、なりすました音声を再生したりすることにより、命令を誤認識させることができる可能性もある。中には、図２に示すように特定の狭い方位のみに音波を発信する指向性のスピーカーを用い、周囲にいる正当な利用者には気づかれないようにスマートスピーカーを悪用する巧妙な攻撃の可能性も指摘されている。

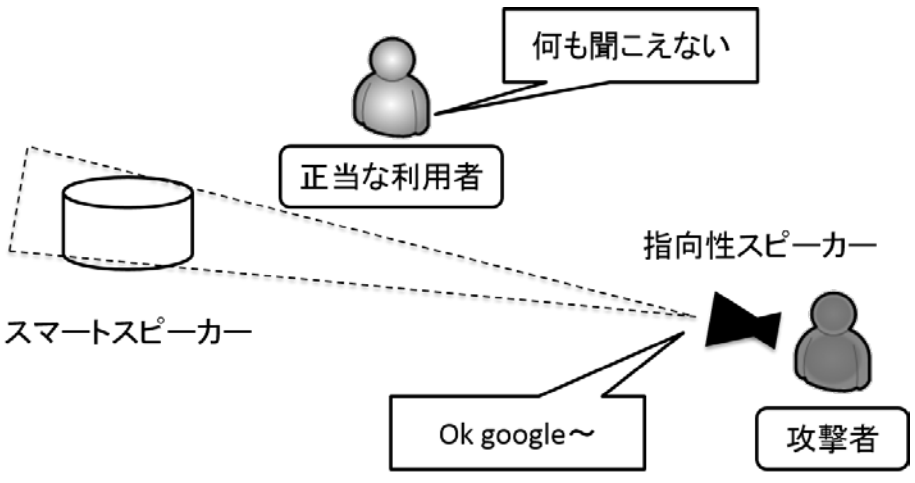

図２：指向性スピーカーを用いた攻撃

その他のセンサも同様に、偽の信号等を照射することにより、機器を無力化したり、状態を誤認識させたりすることができる可能性がある。

アクティブ方式のセンサに対しても同様に、それぞれのセンサに対して物体の測位を不能としたり、位置を誤認識させたりする攻撃が考えられる。アクティブ方式のセンサは、主として物体の測位を目的としている。そのため、その攻撃手法としては測位対象の物体に何らかの細工を施す攻撃が考えられる。例えば、電波の反射面積を小さくしたり、様々な方向に乱反射させたり、あるいは電波を吸収する素材を用いたりすることにより、測位を無力化することができる可能性がある。これらの手法は、軍事分野においてはステルス技術として古くから知られている。別の攻撃手法としては、パッシブ方式のセンサに対する攻撃と同様に、反射波等を偽装する攻撃が考えられる。ただし、センサに対して電波等を照射する点は共通であるが、アクティブ方式ではセンサ自身が照射した電波等の反射波等の影響を考慮する必要がある。図３にアクティブ方式のセンサである測距レーダーへの攻撃の例を示す。

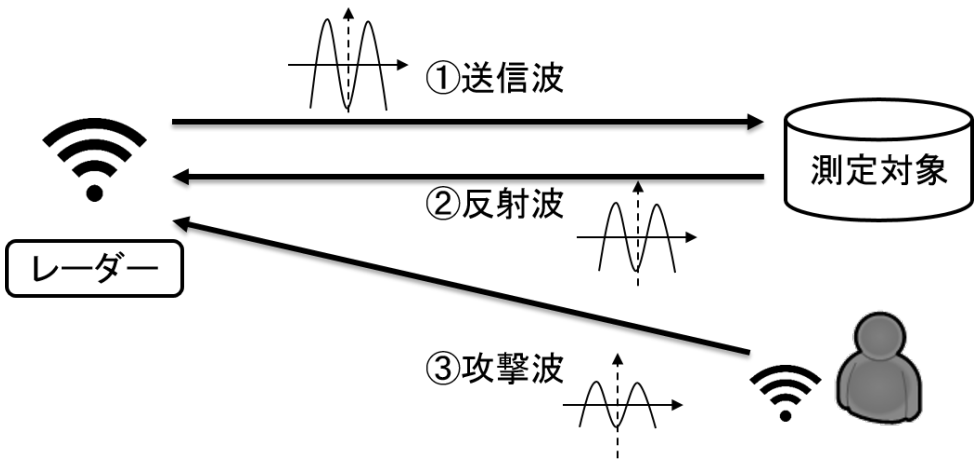

図３：測距レーダーへの攻撃の例

この例では、レーダーで捜索用の電波（図３①）を一定の周期で発信し、物体からの反射波（図３②）をセンサで観測し、その物体の位置を測定している。ここで、そのセンサに単純に同一の周期で偽装した攻撃波（図３③）を照射した場合、反射波と偽装した攻撃波の合成波がセンサで観測される。そのため、その合成波がうまく意図した波形となるように照射する電波の波形を調整する必要がある。合成波の波形を得るためには、反射波と照射する攻撃波の波形が必要となる。ここで、照射する攻撃波（図３③）は攻撃者が制御することができる。したがって、反射波（図３②）の波形を得るためにセンサが発信した電波（図３①）を分析する器材も必要となる。このように、アクティブ方式のセンサに対しては、反射波等の影響を考慮して電波等を照射することにより、物体の位置を誤認識させることができる可能性がある。

５　センサへの攻撃の対策

（１）内部ネットワークからの攻撃への対策

内部ネットワークからの攻撃は、内部ネットワークというサイバー空間において実施される攻撃であるため、その手法は伝統的なサイバー攻撃と類似している。したがって、その対策にも多くの伝統的なサイバー攻撃への対策手法を応用することが可能である。

攻撃者は内部ネットワークに接続するノードの制御を奪うために、ＵＳＢポート、赤外線ポート、無線ネットワーク等の正当な通信手段を介してアクセスする場合が多い。そのため、それらの正当な通信手段において、適切なアクセス制御を実施することが最も基本的な対策となる。また、内部ネットワークに接続するノードが制御を奪われないように、ノード自身の脆弱性をなくすことも重要である。しかしながら、インターネットの常時接続していない機器や、運用を停止することが困難な機器については、アップデートによう脆弱性の修正が困難である点には注意を要する。

攻撃者は、内部ネットワークに接続するノードの制御を奪うと、そのノードを起点として内部のネットワークのトラフィックを監視し、メッセージを盗聴したり、あるいは改ざんや偽のメッセージを送信したりすることが可能となる。このような攻撃に対しては、通信内容を暗号化して盗聴を防止したり、認証技術を用いて改ざんや偽のメッセージを検知したりすることが可能である。また、内部ネットワークのケーブルの盗聴、不正な機器の接続等を防止するために、ネットワークケーブルやケーブルのポートを物理的に保護するといった物理的な対策も重要である。

（２）外部からの攻撃への対策

外部からセンサに対する攻撃への対策としては、主にセンサ自身の耐性の向上と複数のセンサの情報を組み合わせて攻撃を検知するセンサフュージョンが挙げられる。

センサ自身の耐性を向上させる基本的な手法としては、センサへのアクセス制御が挙げられる。例えば、カメラやマイクの電源を不要時には切ることで、攻撃の機会を減らすことが可能である。しかしながら、これらの機器は常時の使用を前提としていることも多いため、このような対策は難しい場合も多い。マイクやスマートスピーカーを用いた音声アシスタンス機能では、正当な利用者の声を学習させ、他者の声による命令を受け付けないようにすることで、アクセス制御を実施することができる。このように、センサに対して極力不要なアクセスを制限することは、基本的かつ効果的な対策であると考えられる。

アクティブ方式のセンサに関しては、信号を送信する周期をランダムにする手法が挙げられる。アクティブ方式のセンサに対しては、攻撃者はセンサで観測される反射波等と同じ周期で攻撃波等を照射する必要があるため、送信波のタイミングを知る必要がある。仮に攻撃者がこの周期を無視した場合には、セ

ンサ側で周期に合致しない信号を遮断することで、アクセス制御を実施することが可能である。このように、送信波の周期が分からなければ、攻撃者が信号を偽装することは難しくなる。このような対策の基本的な考え方は、軍事分野においてはレーダー等へのジャミング対策として古くから知られている周波数ホッピングと同様である。

次に、もうひとつの対策であるセンサフュージョンについて説明する。センサフュージョンでは、主に複数のセンサから得られる情報に着目し、統計的な手法を用いて異常を検知することが可能である。図４にドローンのセンサフュージョンの例を示す。

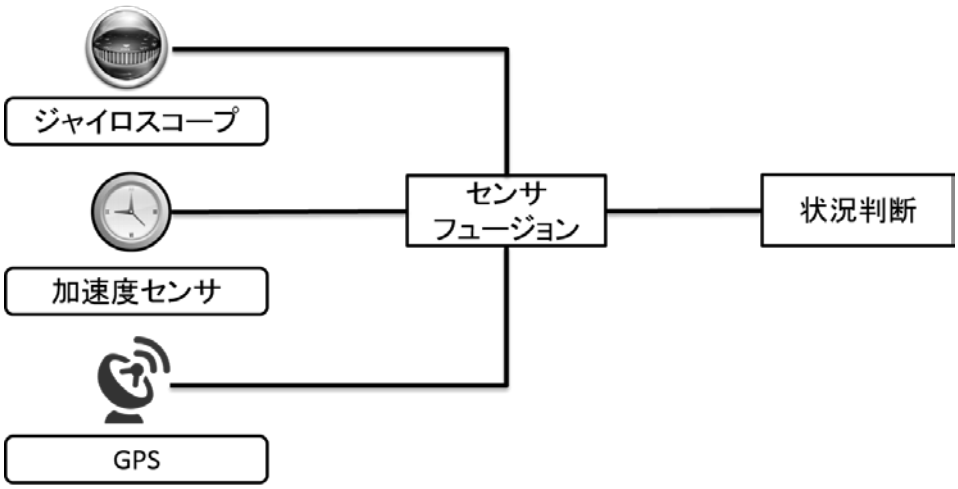

図４：ドローンのセンサフュージョンの例

この例では、ドローンはジャイロスコープ、加速度センサ及びＧＰＳから情報を取得し、それらの情報をセンサフュージョンで統合し、状況判断を実施している。ここで、ＧＰＳに偽の位置情報を認識させる攻撃について検討する。この攻撃は、暗号化されていない商用のＧＰＳに対して有効であり、ソフトウェア無線機を用いて信号を偽装することで実施することが可能である。このような攻撃に対しては、ＧＰＳから得られる電波の強度や位置情報を継続的に監視し、その時系列のデータから予測値を算出して現在値と比較することで、異常を検知することが可能である。位置情報であれば、最大速度から移動可能範囲を算出し、過去の位置からおおよその現在位置の範囲を推定することができる。図５にＧＰＳの信号偽装の対策の例を示す。

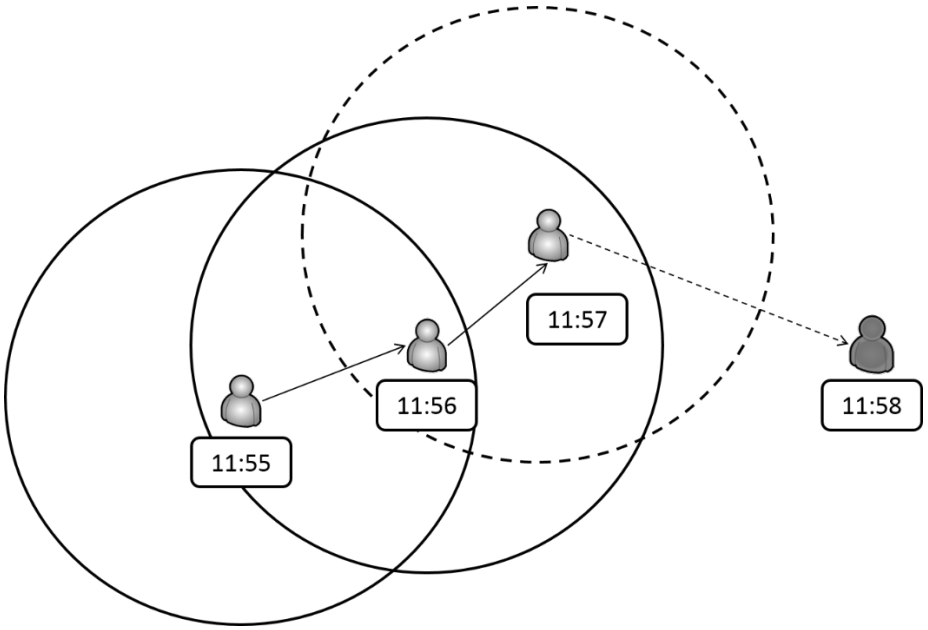

図５：ＧＰＳの信号偽装の対策の例

図中の人物のアイコンはその時刻における位置、矢印は移動経路、円は移動速度を考慮した移動可能範囲を示す。ここで、ＧＰＳから得られる現在位置が、移動可能範囲内にない場合には異常と判断する。例えば、１１：５５～１１：５７の間の位置は移動可能範囲内であるが、１１：５８の位置はその範囲（図５破線）を外れているため、偽装攻撃を受けたものと判断する。換言すると、ＧＰＳから得られる位置情報の変化が、想定した範囲内であるかを確認していることになる。もちろんこのような手法では、攻撃者が想定の範囲内で位置情報を偽装した巧妙な攻撃を検知することはできない。そこで、ジャイロスコープ、加速度センサ等の複数のセンサの情報を組み合わせて照合し、その信頼性を高める手法が提案されている。例えば、ＧＰＳから位置情報が使用できなくなったとしても、ジャイロスコープ、加速度センサ等の他のセンサからの情報を用いて移動距離を計算し、現在地を予測することもできる。この予測した現在地とＧＰＳからの位置情報を比較することで、異常を検知することも可能である。

６　おわりに

本稿では、センサ・セキュリティに関する具体的な事例について述べ、主にＩｏＴ機器に搭載されるセンサの役割について説明した。さらに、センサへの攻撃を体系的に整理し、各攻撃に対する基本的な対策の概要について説明した。

今後、ＩｏＴ機器はますます普及し、あらゆるモノがスマート化することが予想される。自動車の自動運転サービスや無人機もますます普及し、音声アシスタンス機能を用いたより高度で利便性の高いサービスも次々と開発されている。計算機性能の向上や機械学習技術の発展は人工知能分野を加速し、従来は人間にし

かできないと考えられていた様々なタスクが自動化されようとしている。現在は人間のパイロットが操縦している航空機や、他のあらゆる乗り物が無人化される可能性は高い。このような状況において、スマート機器の目や耳の役割を果たすセンサは非常に重要である。センサが正常に動作しなければ、スマート機器が正常に現状を認識し、自律的なサービスを提供することは不可能である。さらに、悪意ある攻撃者によって利用者が意図しない動作をする危険性もある。例えば、ＷｉｋｉＬｅａｋｓによって暴露されたＶａｕｌｔ７[17]と呼ばれるＣＩＡの内部文書によると、高度に自動化された車の追跡やハッキングが検討されていたとされている。その目的は明示されていないが、意図的に事故を起こさせて要人を暗殺する用途ではないかと推測されている。例えば、米国や欧州で装着が義務化されているＴＰＭＳ[18]と呼ばれるタイヤの監視システムが発する電波を傍受すれば、遠隔で特定の車を識別することが可能である。このようにして特定の車を識別し、さらにその車のセンサに干渉して誤操作を誘引することにより、意図的に交通事故を起こさせるといったシナリオも考えられる。

また、センサ・セキュリティの問題は軍事分野にも密接に関係している。センサへの攻撃や対策でも示したとおり、ステルス技術や周波数ホッピングといった伝統的な電子戦の技術には、センサ・セキュリティの分野にも適用できる共通の考え方がある。センサ・セキュリティの問題が伝統的な電子戦と異なるのは、サイバーセキュリティの特性が融合していることである。したがって、無人機が主役となる次世代の戦闘では、このサイバー電子戦とも言える新たなアタックサーフェスを考慮する必要があるものと考える。もちろん、サイバーセキュリティの特性は電子戦以外にもあらゆるドメインに影響しており、ハイブリッド戦あるいは超限戦の重要な要素である。したがって、サイバーセキュリティの素養は、軍事分野に携わる者にとって必須の素養であることに疑いの余地はない。

[17] Vault 7: CIA Hacking Tools Revealed

[18] TPMS (Tire Pressure Monitoring System) 自動車のタイヤの空気圧等を監視するためのシステム