［ハードウェアセキュリティの最新動向］

④ 計測セキュリティ
―サイバー空間と物理空間のつなぎ目における脅威とその対策―

松本　勉 | 産業技術総合研究所　鈴木大輔 | 産業技術総合研究所

計測セキュリティとは

計測セキュリティは，CPS（Cyber Physical Systems）やIoT（Internet of Things）の特徴である，物理空間から収集した情報をサイバー空間で扱う際に発生する脅威へ対抗するための技術である．計測セキュリティについて解説する前に，CPS/IoTのシステム構成について外観について概観してみよう．CPS/IoTの典型的なシステム構成を図-1に示す．構成要素としては，まず物理空間の情報を収集するセンサを搭載した機器がシステムの末端に必ず存在する．次にその機器はゲートウェイを経由してクラウドに接続される．そしてゲートウェイあるいはクラウドでは，収集した情報に対する分析処理を行い，その結果は機器へフィードバックされ，機器が持つアクチュエータの制御に用いられる．このようにCPS/IoTは，センサから情報を収集し，アクチュエータの制御が行われるまでの大きなループをデータが循環するシステムと言える．

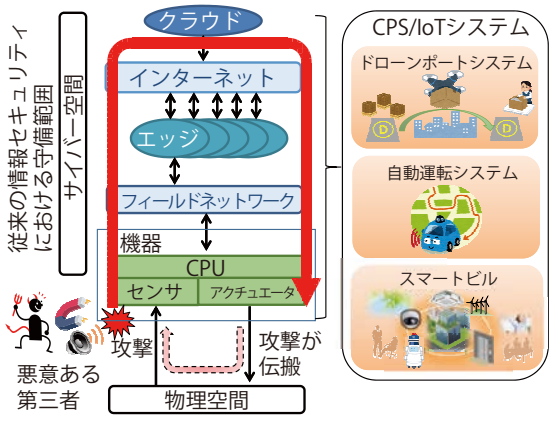

図-1　CPS/IoTのシステム構成と計測セキュリティ

計測セキュリティは，末端のセンサに対して意図的な攻撃を行う悪意ある第三者を仮定し，どのような攻撃が可能か，その攻撃に対してはどのような対策が可能かを，実際にその脅威が現実となる前に先回りして研究している分野である．したがって，攻撃方法としては「そこまでやるのか」と思われる方法が数多く存在するが，それらの攻撃は技術の進歩によって，現実的な攻撃に発展する可能性があることを研究者間では（暗黙的に）共有しており，手段を制限せずさまざまなアプローチで研究が行われている．

具体的なイメージをつかんでもらうために，計測セキュリティが扱う脅威の例をいくつか挙げる．たとえば，自動運転システムにおいて，外界環境をセンシングするための車載センサが攻撃されることによって，事故などの人命にかかわるリスクが発生する可能性がある．あるいは自律運転中のドローンが持つ姿勢センサに対する攻撃は，ドローンの落下事故につながるかもしれない．スマートスピーカのマイクへの攻撃によって，家の外からいつの間にか情報家電が操作されるかもしれない．以上に挙げたような攻撃は，すでに実製品を用いて概念実証が示されたシナリオである．

このように，センサを利活用した新しいシステムの普及に伴い，センサを狙った攻撃に関する脅威が深刻化する恐れがある．本稿では，さまざまなアプローチが示されているセンサへの攻撃を整理し，セキュアなシステム設計にフィードバックする上での課題を探る．

計測セキュリティの研究事例

自動運転や自律型ロボット等の自律システムでは，センサ情報をリアルタイムに処理するのでセンサへの攻撃がシステムに与える影響を注視する必要がある．そこで本章では図-1の一形態として図-2（a）に示すセンサを用いた自律システムのモデルでセンサへの攻撃を整理する．図-2（a）のモデルは，センサ情報を用いた認知・判断と制御機能を担うコントローラと動的な特性を持つシステムから構成される．人が介在するシステムでは人がコントローラへの目標値を入力するが，自律システムではセンサを用いた周辺計測と，その計測値に対する認知・判断の処理で目標値を算出する．また，センサはフィードバック制御を行うためにシステムの状態を計測するためにも用いられる．以下の節では，この自律システムに対するセンサへの攻撃を「攻撃対象のセンサ」，「攻撃に用いる媒体」，「計測値への影響」，の3つの視点から整理する．

攻撃対象のセンサ

図-2（b）の青枠に示されるさまざまなセンサが攻撃対象となっている．攻撃対象のセンサは，大別して能動型と受動型に分類できる．能動型とは，LiDAR（レーザを用いた測距センサ）やレーダなどセンサ自身が出したエネルギーの反射を計測する仕組みを持つセンサを指す．これらのセンサは，図-2（a）で周辺計測に用いられることが多い．受動型は，ジャイロセンサやマイクなど計測対象から発せられるエネルギーを受信するだけの仕組みを持つセンサを指す．これらのセンサは，図-2（a）で状態計測に用いられることが多い．ただし，この分類は必ずしも厳密ではない．たとえば，イメージセンサ（カメラ）は計測の方式によって能動型と受動型が混在する．また，GPSは受信機単体で見れば受動的に見えるが，システム全体としては能動的である．

ここで重要なポイントとしては，次に説明する攻撃に用いる媒体との関係である．センサが計測で用いる媒体は真っ先に攻撃にも利用される可能性がある．たとえば，レーダであれば自身が用いる帯域と同じ電波が，マイクであれば再生可能な周波数帯域の音が攻撃に利用できる．さらに興味深いのは，センサが用いる媒体とは異なる媒体を用いた攻撃事例

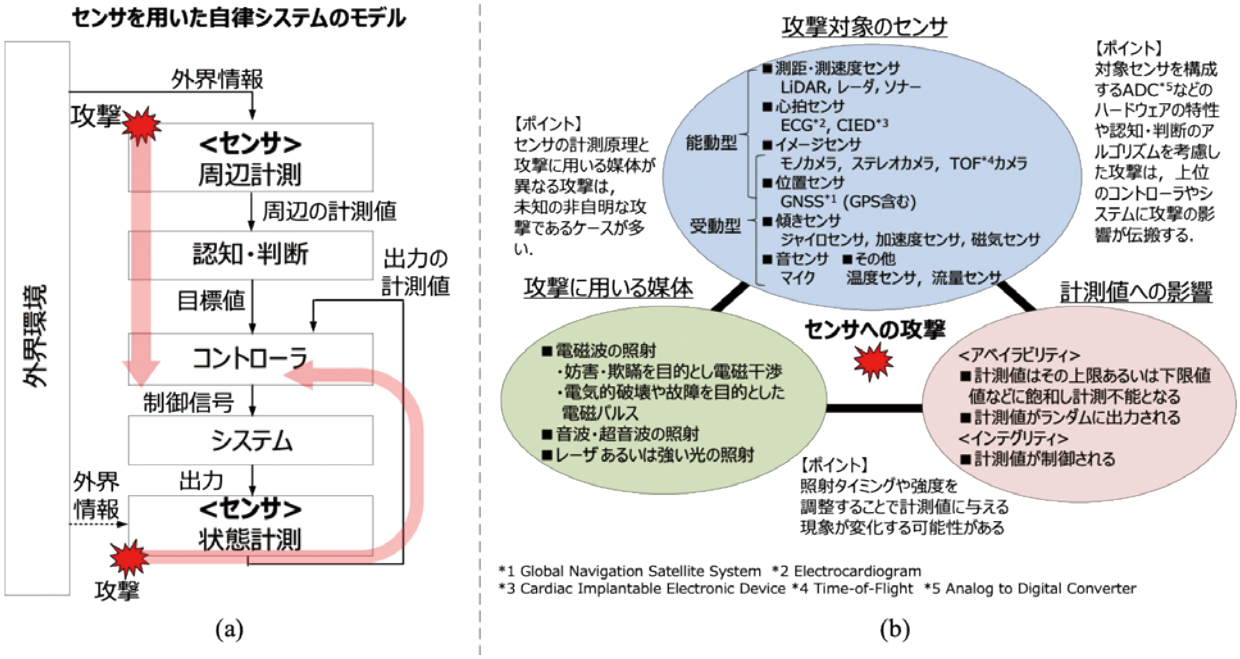

図-2 センサに対する攻撃の全体像

が多数報告されている点である．たとえば，加速度センサに超音波を照射する攻撃や，マイクにレーザを照射する攻撃である．このように，さまざまな視点から攻撃の可能性を探る研究が行われている．

攻撃に用いる媒体

攻撃に用いる代表的な媒体を，図-2（b）の緑枠に示す．電磁波，音波，超音波，レーザあるいは強い光の照射などによる攻撃が知られている．これらは単純な照射にとどまらない．照射が計測値に与える影響を詳しく分析し，照射時に適切な変調を加えることで，最終的には計測値を自由に制御可能な事例が報告されている．また，同時に複数の媒体を用いて高度な制御を行う攻撃が存在する．例として，文献1）ではジャイロセンサや加速度センサに超音波を照射することで計測値を狂わせる攻撃が示されている．これは，MEMSセンサ（微細な機械要素と電子回路を利用したセンサ）のばね・重り構造が共振周波数を持つためである．照射時にセンサ内のアンプやローパスフィルタの特性を考慮して照射する超音波に振幅や位相変調を加えることで，計測値をコントロールできる．

計測値への影響

攻撃が計測値に与える影響は図-2（b）の赤枠に示すように「アベイラビリティ」と「インテグリティ」の2つのケースに大別できる．カメラが強い光によってホワイトアウトする現象などの計測値が上限値あるいは下限値などに飽和するケースや，レーダに対するジャミングのように計測値がでたらめな値を示すケースは，アベイラビリティに影響を及ぼす攻撃である．一方で，前述した変調を加えた超音波の照射のように，計測値を制御できる攻撃は，別の物理現象を計測したように「なりすまし」が可能なことを意味する．すなわちこれはインテグリティに影響を与える攻撃と言える．

脅威としては，インテグリティを脅かす攻撃が深刻である．アベイラビリティの侵害も同じく深刻な脅威であるものの，センサが故障する脅威と同じ影響と考えることができるため，システムの信頼性の観点で織り込み済みであることを期待できる．また，計測できないことはシステムとしては検知しやすいため，対処しやすい．以上から，完全性を脅かす攻撃，たとえばシステムが気が付かないうちにセンサの計測結果が操作されている攻撃が，計測セキュリティで扱う重要な脅威と言える．

前述の通り，この攻撃の影響範囲はセンサだけにとどまらない．図-2（a）において認知・判断のアルゴリズムを考慮してセンサを攻撃することで周辺の計測値を制御し，認知・判断の出力である目標値を攻撃者にとって都合のよい値にすることができれば，センサへの攻撃でコントローラやシステムにまで影響を与えることができる．また，図-2（a）で出力の計測値を制御できれば同様の現象を引き起こすことができる．つまり，自律システムではセンサへの攻撃がシステム全体に波及する可能性があるため，その影響を見極める技術が重要となる．

最近の研究成果では，センサ情報に対して認知・判断のアルゴリズムとしてニューラルネットワークを導入するケースにおいて，ニューラルネットワークの不具合を狙うことで攻撃が可能となる事例が報告されている．文献2）の「敵対的パッチ」と呼ばれる特殊な模様をカメラが撮像すると，図-3のように人の検出が無効化することが知られている．これはセンサ情報に対して計測後にどのような処理が行われるかを考慮した攻撃事例と言える．このほかにも，ノイズ対策のためのカルマンフィルタによるセンサフュージョンを突破可能なセンサ攻撃が示されており[3]，計測の後段にノイズに頑健な処理があっても攻撃の影響がシステムへ貫通することが示唆されている．

図-3　歩行者検知における敵対的パッチの影響

計測セキュリティの保証に向けて

私たちの目指すべき目標は，セキュアなCPS/IoTシステムを構築することである．しかし，目標に至るまでにはまだ多くの課題がある．本稿で挙げる課題の概略を図-4に示す．

課題1：各ドメインでの影響評価

第一に，計測セキュリティは黎明期にあるため，現状では毎年新な攻撃方法が学会等で発表されている．その一方で，それらの攻撃が電力，ビル，FA/PA，自動車など各ドメインのシステムにどの程度の影響を及ぼすのか，判断する手段はほとんど存在していない．論文として公知になる攻撃に関する研究は，固有の実験環境での概念実証であるため，簡単に再現できない．攻撃方法を広く共有し，各ドメインにおけるセンサの用途において攻撃の影響を議論できる枠組みが必要である．このためには攻撃環境の共有や，攻撃方法をシミュレーション可能なモデルとして共有するアプローチが考えられる．

課題2：強化技術と評価技術

第二に，センサへの攻撃がシステムにとって影響を及ぼすのであれば，対抗するためのセキュリティ強化技術が必要となる．また，その有効性を定量化するための評価技術が必要となる．ここで，センサや機器単体でセンサへの攻撃に対抗すべきかは議論の余地がある．攻撃とシステム構成によっては，ゲートウェイやクラウドで効果的な対策が打てるかもしれない．このようにシステムのアーキテクチャの中で，各構成要素がどこまでのセキュリティを担保するのか効果的な対策のアーキテクチャに関する研究が今後必要となる．

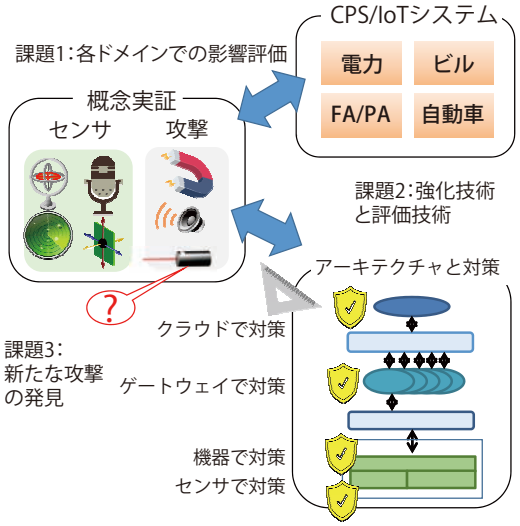

図-4　計測セキュリティの課題

課題3：新たな攻撃の発見

第三に，システムには多種多様なセンサが組み込まれることから，先回りして新たな攻撃，すなわち脆弱性の評価方法を発見することが重要である．予期せぬ攻撃への対策は難しい．計測セキュリティは，センサやアナログ回路から信号処理，システムのアーキクチャなどさまざまな視点で攻撃者の立場で考える必要があるため，「高い攻撃力」を持った人材の育成が必要である．

これらの課題解決を通して，各ドメインでシステムのユーザとベンダの双方が計測セキュリティの視点で要求事項や要求水準が満たされていることを相互に確認できる「セキュリティ保証」の枠組みを確立していく必要がある．

参考文献

1) Trippel, T., Weisse, O., Xu, W., Honeyman, P. and Fu, K. : WALNUT : Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks, IEEE European Symposium on Security and Privacy (EuroS&P) (2017).
2) Thys, S., Ranst, W. and Goedeme, T. : Fooling Automated Surveillance Cameras : Adversarial Patches to Attack Person Detection, arXiv preprint arXiv:1904.08653 (2019).
3) Nashimoto, S., Suzuki, D., Sugawara, T. and Sakiyama, K. : Sensor CON-Fusion : Defeating Kalmanlter in Signal Injection Attack, ACM ASIA Conference on Computer and Communications Security (ASIACCS) (2018).

(2020年2月4日受付)

松本　勉　matsumoto.tsutomu@aist.go.jp

1986年東大大学院工学系研究科博士課程修了，博士（工学）．現在，横浜国大教授および産総研サイバーフィジカルセキュリティ研究センター長．国際暗号学会元理事．電子情報通信学会業績賞，ドコモ・モバイル・サイエンス賞，文部科学大臣表彰・科学技術賞等各受賞．

鈴木大輔　suzuki.daisuke@aist.go.jp

2001年東京理大理工学研究科博士課程前期修了，2011年横浜国立大学大学院環境情報学府博士課程後期修了，博士（工学）．2001年から現在まで三菱電機（株）でセキュリティ技術の研究開発に従事．2019年から産総研客員研究員．