# 第 132 回　大阪大学工業会機械工学系　技術交流会

## 自律駆動型インフラ時代を支える機械システムセキュリティの最前線

**キーワード**:フィジカル AI、重要インフラ、サイバーセキュリティ、制御システムセキュリティ、センサセキュリティ、オフェンシブセキュリティ、 制御工学、信号処理、機械学習

**【趣旨】**

自動運転やスマートインフラに代表される自律駆動型社会の裏側では、機械システムを狙うサイバー脅威が巧妙化し続けています。本講演会では、歴史・理論・実践の 3 要素から次世代のシステム防衛のあり方をお伝えします。学術的な深み（理論）と製品開発への知見（実践）が融合する講演です。皆様のご参加を心よりお待ちしております。

【歴史】 Stuxnet が変えたセキュリティのパラダイムに触れ、IT セキュリティの常識を覆し、物理インフラの防御へと評価対象を急激に広げた黎明期を紐解きます。

【理論】 機械工学のコア学問である制御工学を通して実現する、「破られないシステム」のための「新しい数理モデル・制御理論」アプローチを解説します。

【実践・応用】 自動車、データセンター、スマートデバイス等に対する最新脅威に対し、攻撃者の思考プロセスを逆手にとって脆弱性を先回りして排除する実践的な手法を提示します。

記

日　時: 2026 年 12 月 4 日（金） 13:30 ～ 17:00

会　場: 大阪大学大学院工学研究科機械工学専攻

M4 棟 2 階 201 講義室

http://www2.mech.eng.osaka-u.ac.jp/access/

----------《スケジュール》----------

13:00～　　開場・受付

13:30～13:35　会長挨拶　大阪大学 大学院工学研究科 教授 小林 英樹 氏

13:35～14:30　講演1:**「機械システムからみたサイバーセキュリティ:縮退と回復」**

大阪大学 大学院工学研究科 教授 澤田 賢治 氏

14:30～14:50　コーヒーブレイク

14:50～15:50　講演2:**「敵対と欺瞞をめぐる制御理論:ダイナミクスに潜む機械システムの脆弱性」**

東京大学 大学院情報理工学系研究科 講師 笹原 帆平 氏

15:50～16:00　小休憩

16:00～17:00　講演3:**「アナログ領域でセンサをあざむく攻撃:フィジカル AI 時代の新たな脅威」**

電気通信大学 大学院情報理工学研究科 准教授 菅原 健 氏



講演概要、次ページへ

----------《講演概要》----------

**講演1の概要**:

近年、サイバー攻撃の被害対象は拡大し続けている。IT システムにおける個人情報漏洩や情報改ざんは勿論のこと、ガス・水道・電気・通信・医療などの重要インフラ 16 分野におけるサイバー脅威は留まるところを知らず、ほぼ毎日何らかのインシデントが報告されている。特に、自動車、鉄道、航空など「動くもの」を守るには、従来の IT セキュリティの考え方だけでは不十分である。本講演では、2010 年の制御システム向けマルウェア Stuxnet によるイラン核燃料施設への攻撃が、機械システムに対するセキュリティ意識をどのように変えたのか、そして何を変えなかったのか、講演者の視点で振り返る。本講演は、講演者の当時の失敗談を中心にして、機械工学分野の研究者が機械システムのサイバーセキュリティ対策研究を始めるのにどこで躓いたのか、何処から研究を始めなければならなかったのかを解説する。時間が許すならば、失敗と試行錯誤の中で研究を続けてきたサイバーセキュリティ対策としての縮退制御と回復制御についても解説する。

**講演2の概要**:

自動運転やスマートインフラに代表される機械システムでは、データを狙ったサイバー攻撃が物理的な挙動を変え、安全性を脅かす。本講演では、意思を持つ敵対者やその認識・判断への働きかけを扱う「敵対と欺瞞をめぐる制御理論」の立場から、機械のダイナミクスに潜む脆弱性を解説する。まず、制御システムセキュリティの背景を概観し、運用時と設計時という二つの段階におけるデータ改ざん攻撃を取り上げる。運用時については、制御理論に基づく既存研究の代表例として、観測上は異常が現れないまま内部状態を変化させる攻撃を紹介し、ダイナミクスと検知の限界との関係を示す。続いて、講演者らが取り組む設計時の攻撃の研究として、設計用データの改ざんによる制御系の不安定化や、特定の条件で危険な挙動を引き起こすバックドアを紹介し、自動運転を対象とした検証と防御への展開を述べる。これらを通じて、攻撃の仕組みを理解し、安全な機械システムを設計するために制御理論が果たす役割を示す。最後に、知覚と制御が連携する Physical AI のセキュリティについて、講演者自身の今後の研究展望を述べる。

**講演3の概要**:

自動車やロボットがセンサを通じて実世界を認識し、自律的に行動する「フィジカル AI」の社会実装が急速に進んでいる。一方で、光・音波・電磁波などを照射して物理層からセンサに誤った情報を注入する、新たな攻撃の脅威が顕在化している。デジタル情報に変換される前のアナログ信号を守るセキュリティ技術は、従来にない新たな研究分野として過去 10 年間で急速に発展してきたものの、未だ発展途上にある。講演者はこの分野で、未知の脅威を能動的に発見するオフェンシブセキュリティの方法論に基づいて研究を進めてきた。本講演では、その成果を交えながら、センサシステムにおいて攻撃の起点となりうる箇所を 3 つの層に分けて解説する。第 1 はセンサの物理層である。ここでは、センサが本来の計測対象とは異なる物理量にも反応してしまう性質を悪用する攻撃を取り上げる。第 2 は信号処理層である。前処理やキャリブレーションなどの処理が意図しない副作用を生み、攻撃の足がかりとなりうることを示す。第 3 は機械学習層である。敵対的サンプル（Adversarial Example）に代表されるように、人間には気づかれない、あるいは無害に見えるわずかな変化が、機械学習モデルの判断を大きく誤らせることがある。

以上