次世代制御システムにおけるサイバーセキュリティとレジリエンスの確立

機械工学専攻　知能制御学系
機械情報システム制御学領域
教授　澤田　賢治

1.　はじめに

2025 年 4 月に工学研究科機械工学専攻知能制御学講座機械情報システム制御学領域に着任いたしました．2000 年 4 月に工学部応用理工学科に入学し，その後，2003 年 4 月に池田雅夫教授の研究室（制御工学領域）に配属されました．もともと大学には学位取得を目的に進学していたため，大学院も制御工学領域が所属する電子制御機械工学専攻に進学しました．途中，2005 年に電子制御機械工学専攻を含めた機械系 3 専攻が 4 部門体制の機械工学専攻に統合され，2009 年 3 月に機械工学専攻知能制御学部門にて博士（工学）を取得しました．翌月 4 月からは東京都調布市にある電気通信大学電気通信学部システム工学科数理システム講座の新誠一教授の研究室に助教として着任し，途中，2015 年 2 月に准教授に昇任しながら，16 年間同大学で教育研究を行ってきました．

もともと兵庫県の出身で，大阪大学で学位を取得するまで，自分が東京に異動することになるとは思いもよりませんでした．電気通信大学での 16 年間は，関西と関東の文化的な違い，東京における情報展開の速さ，所属大学の 3 回の改組，大講座制での単独研究室運営など，あっという間の期間でした．この一連のカルチャーショックは自分の研究テーマに大きな影響を与えました．そしてこのたび，大変光栄なことに，出身専攻である機械工学専攻にて教育研究を行う機会を頂きました．学部・大学院とご指導いただきました池田雅夫先生（現名誉教授）の制御工学領域を直接引き継ぐなどと大層なことを言えるわけではありませんが，新時代の制御工学の発展を促す新しい領域として，機械情報システム制御学領域を運営していきたいと思っております．

私はこれまで，制御工学を専門とし，最適化理論や情報理論といった数理工学と融合した制御理論の構築，さらにはサイバーセキュリティ，エネルギー，自動運転，情報家電，産業機器など多様な分野への応用を行ってきました．電気通信大学という比較的コンパクトな大学で，かつ周辺に様々な有名大学がある中で，研究のインパクトを高めるために，1 つのことを極めつつも，多様なことに挑戦することを戦略としてきました．それと同時に，個別にはばらばらに見えても，問題ごとに適用する手段が違うだけで，目指すのは安心安全な社会を支える機械システムの創出であると考えてきました．

2.　制御システムのサイバーセキュリティとレジリエンス

本稿で紹介するのは，私の研究テーマの 1 つの大きな柱である制御システムのサイバーセキュリティです．2020 年以降，様々な情報システムに加え，生産工場やインフラシステムに対するサイバー攻撃の報道頻度が増加しました．Windows マシンやインターネットプロトコルといった汎用的な情報技術の進歩が加速したことから，2000 年前後から私たちのライフラインを支える重要インフラの制御システムにおいても情報化やネットワーク化が進んでいます．それと同時に，情報漏洩，サイバー攻撃，ウイルス感染などが制御システムでも発生するようになりました．特に世界的に影響を与えたのは，2010 年のイラン核燃料施設へのサイバー攻撃，いわゆる STUXNET 事件です．この事件を契機に，私は制御システムのサイバーセキュリティ研究に本格的に取り組むようになりました．産業インフラが標的となったこの攻撃は世界に衝撃

を与え，日本でも経済産業省や IPA を中心にセキュリティ対策活動が加速しました．その流れの中で，私は 2011 年に国内の委員会に参加し，海外との相互認証制度の検討や，技術研究組合制御システムセキュリティセンターの設立などにも関わることとなりました．

制御システムのサイバーセキュリティ研究では，縮退運転システムを研究しています．制御システムから脆弱性を完全に排除することは困難であるという前提に立ち，攻撃者の優位性を削ぐ仕組みとして設計したものです．制御システムの制御器の入出力装置とアクチュエータやセンサなどのフィールド機器の間にセキュリティ機器を設置し，攻撃を受けてもシステムが完全に停止せず継続的に運用できることを目指しました．模擬プラントでの実証や企業との共同研究を通じて，その有効性を確認することができました．

また，協調型セーフリストの開発にも取り組みました（図 1）．パソコンなどに導入されているセキュリティ機能は「ウイルスに代表される特定の不正な動きを検知する」ブロックリスト方式です．本研究では，セキュリティ機能が制御システム本来の機能を阻害しないように，「登録されている正常な動きだけを許可する」セーフリスト方式の開発に注力しました．従来のセーフリスト方式はなりすまし攻撃に弱いという課題がありましたが，私たちのチームは国家プロジェクト SIP「重要インフラにおけるサイバーセキュリティ確保」に参画し，STUXNET のような高度なマルウェアにも対応できる仕組みを開発しました．2020 年には社会実装段階に到達し，水道事業体の水道制御システムに制御器用のセーフリスト方式を試験導入することで，実環境での有効性を示しました．これに関連して，制御オペレータに対するサイバーセキュリティ演習を展開し，社会実装の深化に努めています．

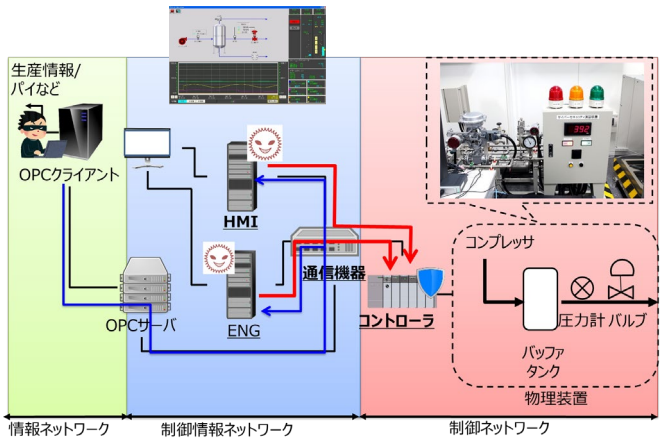

図 1　ガス制御システムへの協調型セーフリスト実装

私は別の研究テーマとして自動車の制御技術の開発を行ってきましたが，2021 年以降は自動運転車両のためのセキュリティ機能開発にも注力しています．自動運転では，制御ロジックだけでなく，センサや AI による認識・判断までも含めた総合的なセキュリティが求められます．私は，サイバー攻撃を受けても安全に走行を継続できる仕組みを目指し，統合的な防御技術の研究を進めています．

3.　おわりに

制御システムは社会基盤を支える横断的技術であり，そのセキュリティは人々の安全・安心と直結します．複雑化する社会システムのセキュリティ問題は，1 つの事柄に特化した技術だけでは本質的な解決が難しい状況です．この事実に加えて，研究室の英語名「Mechanical Informatics and Systems Control Subarea」から，私は研究室の略称名を MISC Lab としています．MISC という単語には「その他」「種々雑多なもの」「寄せ集め」といった意味があります．私は MISC を「多様な事柄・事象」や「既存のカテゴリーに当てはまらないもの」として捉え，そうしたものから制御の本質を取り出し，新たな機械システムの革新を生み出し，社会システムのセキュリティ問題を解決することを大阪大学着任後の MISC Lab のテーマとして掲げることにしました．

最後になりますが，このたびは執筆の機会を頂きましたこと，関係者の皆様に深く感謝いたします．

（大阪大学工学部　応用理工学科　2004 年卒業
大阪大学大学院工学研究科 電子制御機械工学専攻　博士前期課程　2006 年修了
大阪大学大学院工学研究科 機械工学専攻　博士後期課程　2009 年修了）