

七転八倒の制御システムセキュリティ研究者 —「明日からセキュリティの研究をして」から始まった転換点—

随 筆

澤 田 賢 治*

Trials and Tribulations of a Control System Security Researcher:
A Turning Point Beginning with "Start Security Research Tomorrow"

Key Words: Control system security, Automotive control, Industry-academia collaboration

はじめに

兵庫県の出身である筆者は、2000年に大阪大学工学部に入学し、2003年に制御工学の研究室に配属され、博士前期課程、博士後期課程とそのまま進み、2009年3月に機械工学専攻で博士(工学)を取得した。学位論文のテーマはアクチュエータの動作に制限のある機械システムの制御理論の構築である。機械系でありながら純粋な数理最適化ベースの理論研究であり、学位審査の準備には随分と苦労した記憶がある(図1)。博士後期課程3年次には就職活動としてそれなりの数の大学の助教の公募にトライしたが、面接まで行っても幾度も落とされ、学位審査の準備と相まって、精神的にも辛かった思い出がある。学位審査の時期とほぼ重なる2009年1月頃に公募締め切りのあった東京都調布市の電気通信大学には藁をも掴む思いで書類を送った。とはいえ、公募を出していた研究室の新誠一教授とは全く面識がなかったため、自分が本当に東京で働くことになるとは露ほども思っていなかった。縁とは不思議なもので、2009年4月には電気通信大学に助教として着任し、以来2025年3月までの16年間、関西人として東京で七転八倒することになる。生粋の関西人が関東に移住すれば、カルチャーショックはそれなりにある。エスカレーターで立つ側が逆であることや会話のキャッチボールの違いなどの定番のものは一通り経験し、うどんの出汁は醤油ベースであることも受け入れた。

東京における情報展開の速さには常に驚かされた。関西在住時、日本の中心は(物理的に)関西だと思っていたタイプだったが、関東に来てからはその考えが大きく変わった。各種委員会も共同研究先企業も学会事務局も日帰り圏内にあり、何かが起こればその日のうちに関係者が集まれる。この環境が筆者の研究テーマを大きく変えることになった。文科省が近いからか大学の状況変化も著しく、在職中に所属大学が3回の改組を経験し、筆者の所属も転々としたが、これはまた別の苦労話である。

さて、本稿では、この東京での16年間に経験した制御システムセキュリティと自動車関係の研究の苦労話を書かせていただきたい。



図1 翌年の東京行きを知らない頃 (2008年)

「明日からセキュリティの研究をして」

着任して2年経った2011年4月、当時の上司から冒頭の一言を頂いた。この時期は日本でも海外でも色々な出来事があった。2011年3月は東日本大震災で日本は未曾有の混乱状態であった。津波は非常に痛ましい人的被害は勿論のこと、物流や製造業にも大きなダメージを与えた。また、世界的に見ると、前年2010年の年末頃から2011年初頭は、イランのウラン濃縮施設の遠心分離機を標的としたマルウェア



* Kenji SAWADA

1981年9月生まれ
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)
現在、大阪大学大学院 工学研究科
機械工学専攻 教授 博士(工学)
E-mail: knj.sawada@mech.eng.osaka-u.ac.jp

アStuxnetが発見され、コンピュータウイルスが人の命を脅かす状況に世界が注目していた頃である。この2つの出来事は日本の行政も大きく動かし、経済産業省に制御システムセキュリティ検討タスクフォースが設置された。製造業や物流に加え、電力、水道、ガス、鉄道、通信などの重要インフラの安全・安心を支える制御システムのサイバーセキュリティを世界に先駆けて日本が進める仕組みに繋がるタスクフォースだった。その関連ワーキンググループ(WG)に、右も左も分からぬまま参加することになった。当時は会議書類の中身を確認するのに精一杯で、あまり戦力にはなれていなかった。

そもそも制御理論研究者にとって、サイバーセキュリティの世界では言葉が通じない。研究当初は会話にならない会話が多かった。筆者「制御対象の数理モデルを構築できれば、オブザーバで異常を検知できますよ」。相手「そのオブザーバはどこに設置するのですか」。筆者「制御ではコントローラ側に設置するのが通例ですね」。相手「コントローラ？ ネットワークコントローラのことですか」。筆者「いえ、制御用のコントローラでして」。相手「オブザーバが改竄されない仕組みはどうするのですか?」。筆者「(『ああ言えばこう言う』という状況だった。)」。

制御システムのサイバーセキュリティ自体、当時、誰も正しく実態を把握することは出来なかった。制御、通信、ソフト、サイバーセキュリティ、様々な分野が同じテーブルに座って同じ仕事をしていかなければならない。言葉の壁は用語の定義にも及ぶ。当時、制御システムセキュリティが語られる上で必須単語であったDefense in Depth(多層防御)とLayered Security(多重防御)は、分野によって日本語訳が逆になっていることが普通だった。研究開発を始める前に言葉を揃えなければならない。制御理論の常識が通じない世界で、制御工学の範囲で何ができて何ができないのかを常に意識するようになったのは、今思えばこの時期の収穫であった。

国プロと模擬プラントの日々

2012年には技術研究組合制御システムセキュリティセンター(CSSC)が発足し、宮城県多賀城市に化学プラント、火力発電、ガスなど多種多様な模擬プラント(図2)を備えたテストベッドが整備された。これは世界的にも異例の事態だった。当時、制御シ

ステムセキュリティに対応可能な有数の研究所であった米国のIdaho National Laboratoryですら、模擬プラントは3種類程度だった。筆者は研究者として世界最先端の模擬制御システムで研究に携われることに胸が高鳴った。しかしながら実際には、用語の定義も曖昧な状況だと何を研究すべきか、つまり、制御システムセキュリティとしての問題を見つけるだけで相当な時間が掛かった。機材も検証用ソフトウェアも高価で、脆弱性情報の責任ある開示や機密保持の制約から学生の研究参加も容易ではなかった。結果として、2011年に研究を始めて最初の国際学会発表は2015年である。任期付き助教(任期は2015年1月まで)だった身としては、極めてハイリスクだった。

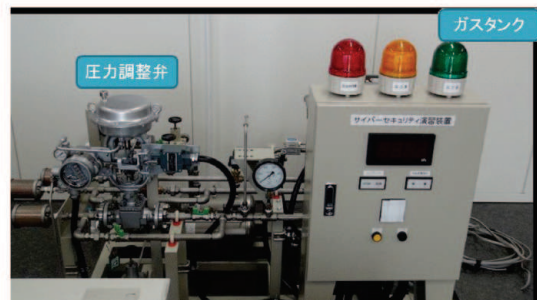


図2 利用頻度の多かったガス模擬プラント

ハイリスクであるからこそ、ハイリターンはあった。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の確保」では、電機メーカー、ネットワーク機器メーカーと連携し、制御端末・ネットワーク・コントローラの3種類のホワイトリストを協調させる防御システムを開発した¹⁾。登録された正常な動きだけを許可するこの方式は制御システムと相性が良く、計測自動制御学会制御部門のパイオニア技術賞を頂くことができた。さらに水道事業体の実際的水道制御システムへの試験導入にも至った。攻撃を受けても完全停止せずに運転を継続する縮退運転システム²⁾の研究と合わせて、制御理論研究者がよくどこまで来られたものだと感慨深い。

貴重な経験

事業体との連携では忘れられない事件がある。ある建屋に最新技術を実装したことをプレスリリースで公開した翌日に同社がサイバー攻撃を受けたとの知らせが届いた。実際には、実装とは全く無関係か

つ何も問題なかったのだが、プレスリリースの扱いは慎重を期すことになった。今でこそ、国内企業におけるサイバー攻撃報道は珍しいものではなく、速やかな公開体制に移れることが1つの社会的信頼性に繋がっている。当時、国内企業の多くは今ほどサイバー攻撃報道に対してオープンではなく、最新攻撃対策導入も隠したいところが多かった。また、制御システムへのサイバー攻撃は「攻撃自体は目立たない一方、結果は甚大である」という厄介な性質を持つため³⁾、対策の価値を企業に説得するには本当に苦労した。



図3 キエフ地下鉄は3路線

2017年前後には、サイバー攻撃による大規模停電を経験したウクライナのキエフまで実情を確かめに行った。その調査過程で、キエフ地下鉄のランサムウェア感染事件の関係者から感染当時の状況と被害時の対応を直接聞くことが出来た。キエフ地下鉄がランサムウェアに感染して中央制御システムが全てダウンした際には、各駅の駅長が電話回線で列車位置を把握して停止と運行を続けたと聞いた。最後にシステムを守るのは人間であるが、そのためにはシンプルなシステム構成も必要であることを思い知った(図3に示す通り、キエフ地下鉄は3路線しかない)。なお、ランサムウェア感染の被害にあった制御用サーバとバックアップ用サーバ、対マルウェア用に更新された運行システムなどを見せてもらったが、あまりのオープンさに、その地下鉄システムの管理棟自体がダミーなのではないかと疑った。

自動車共同研究のおもしろさときびしさ

東京での研究のもう一つの柱が自動車関係である。企業との共同研究開発は、おもしろさときびしさの両方を存分に味わえる世界である。まずはおもしろさから紹介したい。乗用車メーカーとの共同研究開発では、変速機の制振制御や新型パワートレインの開発に長く関わった。乗り心地改善のための振動制

御ロジックは、台車実験から試作車への実装まで至り、その考え方の一部は製品ラインにも反映されていると聞いている。自分が開発に関わった制御ロジックが実車の乗り心地として身体で感じられるのは、研究者冥利に尽きる経験である。近年は自動運転車両で乗員の姿勢自由度が高くなることを見据えた、車酔いを避けるための制御ロジックの開発にも携わっており⁴⁾、制御理論の出番はまだまだ尽きない。

一方のきびしさの筆頭は、成果をすべて表に出せるとは限らないことである。あるメーカーとは複数年間、新型減速機に生じる自励振動の安定化設計に取り組んだ。振動モデルを導出し安定化条件を得て、共同研究開発としては相当に上手くいった。自動車の先行開発は機密度が高く、論文公開できたのは何年も後、メーカーの戦略的な特許整理を待ってからである。大学教員は論文が業績であり、学生には学会発表が晴れ舞台である。この経験から、学生を企業との共同研究開発に参加させる際には、学会発表や論文を前提としたデータ公開のルールを前もって取り決めておくことが常識となった。

既存技術への信頼性から生まれる思い込みのきびしさも経験した。あるトラックメーカーとの共同研究開発では、より顧客のニーズにあったトラックを提供できるようにするために、顧客の長期走行データを圧縮して燃費評価用の走行パターンを作成するプロジェクトに関わった。人手で約3ヶ月掛かっていた作業が3分以内で終わるようになり、機械学習ブームの前にビッグデータの恩恵を実感できた、このプロジェクトも共同研究開発としては大成功の部類である。ところが新しいデータを取るための実車実験の日、大学業務対応で実験場に行けなかった筆者に、実験場に派遣した学生から電話が掛かってきた。「先生、データ解析に使った車両と追加実験の車両が全く違います」。似たような重量のトラックなら、ある程度種類が違って大丈夫だと先方は思ったそうである。確かにそれも正しい推論だが、データ解析時のトラックと追加実験時のトラックは、正面のデザインが違うことから空気抵抗が全く違った。車格が違えば燃費が変わるのは当然であることはお互い共有できていたが、車格が違うとはどういったことなのかまでは共有できていなかった。こちらの常識と相手の常識は違う。成果物の適用範囲まで丁寧に共有すべしという教訓である。

企画開発のスピード競争のきびしさもある。家電メーカーとの共同研究開発で、家電にSNSアカウントを持たせて自身の動作を報告させる「家電の擬人化」システムを開発していた時には、発表を目前に他社に先を越された。なお同じメーカーとは、エアコンが室内環境を自ら学習する省エネ制御を適応制御と外乱推定に基づいて共同開発しており、これは副産物としてエアコンによる室内侵入者検知にも機能する。サイバーセキュリティ研究と家電研究が思わぬところで繋がっている。

共同研究とは通訳業である

ご存じの通り、大学教員の業務は多方面に渡る。論文を定期的に取り、学会運営に関わり、講義を行い、学生を指導する。企業との共同研究開発や国プロは、その合間を縫って進めることになる。そして共同研究開発で求められるのは、研究成果だけではないというのが16年間の実感である。

まず、先方が何を望んでいるのかを知る難しさがある。場合によっては、先方自身も言語化できていない要望を、議論の中からこちらが取り出さなければならない。「困っていることは何ですか」と尋ねて返ってくる答えは、大抵は本当の課題とは限らない。現場の話を聞き、データを眺め、「本当に解くべき問題はこれではないですか」と提示して初めて、共同研究は動き出す。動き出すまでに年単位で掛かる場合もある。相手もプロであり、プライドがある。単なる御用聞きでは務まらず、さりとて理論の押し売りでも務まらない。サイバーセキュリティの会話例で紹介した通り、分野外の人々との会話には通訳が要る。制御の言葉を相手の言葉に翻訳し、相手の言葉を数理の言葉に翻訳する。共同研究開発の成功の秘訣の1つは通訳業にある。

国プロではアウトプットの見せ方にも工夫が要る。学術論文の流儀で成果を語っても、社会実装を求める評価者には届かない。これはSIPに従事しているときも、内閣府関係者から再三指摘された。模擬プラントでのデモンストレーション、実環境への試験導入、事業体オペレータへの演習⁵⁾など、「動くものを見せる」ことに随分と知恵を絞った。シミュレーションで納得して貰えないなら実機で示すしかない。

おわりに

2025年4月、縁あって母校大阪大学の機械工学専攻に教授として着任することができた。16年ぶりの関西である。なお、着任初年度の前期は電通大と阪大の講義を同時に受け持った影響で研究室の引っ越しがままならず、研究室の片付けが完了したのは2026年3月19日であった。

東京での16年を振り返ると、短期的な成果を追い求めるだけでは長期的な成果は得られない、かといって時間は無限にあるわけではない、だからこそ仲間を作ることが重要、というのが偽らざる実感である。失敗はカバーすれば成功に繋がる(時もある)。失敗した時には周りに助けを求める。サイバーセキュリティ研究も自動車研究も、助けてくれる仲間なしにはここまで進めることはできなかった。

大阪大学での新しい研究室の略称はMISC Lab (Mechanical Informatics and Systems Control Subarea) である。MISCという単語には「種々雑多なもの」という意味もある。東京で積み上げた数々の失敗と経験から制御の本質を見だし、安心安全な社会を支える機械システムを創出することを新天地での目標として、筆をおくことにしたい。

参考文献

- 1) 藤田真太郎, 澤田賢治: コントローラホワイトリストの自動化と検証, 計測と制御, Vol. 60, No. 1, 21/26 (2021)
- 2) 澤田賢治: 制御システムセキュリティ技術としてのモデルベース縮退運転システム, システム/制御/情報, Vol. 62, No. 4, 141/146 (2018)
- 3) 澤田賢治, 細川嵩: 制御システムとサイバーフィジカルセキュリティ, 計測と制御, Vol. 58, No. 8, 618/623 (2019)
- 4) 澤田賢治: 制御とモビリティのセキュリティ, 計測技術, 11月号 (2025)
- 5) 澤田賢治, 細川嵩, 榎本真俊, 目黒有輝: スマート保安とセキュリティ教育, 計測技術, 8月号, 6/13 (2024)