



コンピュータ化の喜びと反省

新 誠 一

新 誠一

電気通信大学情報理工学研究所

私の高校生時代、1972年に登場したマイコンはコンピュータ革命とシリコン革命の合流点であった。大学、大学院と専門性を深めていく中で、計測制御機器を始め、家電、自動車などあらゆる機器にマイコンが搭載されていった。21世紀という言葉が少し気恥ずかしい現在ではマイコンが搭載されているスマホ一つで行く先の情報収集、そこまでの道案内、電子乗車券が賄える。それだけでなく、途中で食品や飲料の購入も可能である。もちろん、メールやWebに加えて暇つぶしのゲームにも使える。しかも、子供から大人まで誰でもがスマホを所有している。まことに便利な時代である。

20世紀末までは、あらゆる機器にマイコンを搭載する流れであったように思う。計測制御の分野で使われる専門的な機器への搭載から一般の方々が使われる民生品にマイコン化は進んでいった。それが一段落した2000年頃になると、ネットワーク化の時代変わったように思う。単体のマイコンだけでなく、それらのマイコンをつなぐことで高度な便利さを享受する時代への転換である。

2014年、マイコン化とネットワーク化は既に完成しつつある。一台に100個近いマイコンを搭載した自動車が携帯電話網やVICS (Vehicle Information Communication System) 網を通じて連携している。加えて、マイコンを搭載したテレビ、ビデオ、インターホン、エアコン、冷蔵庫、洗濯機、電子レンジ、電子炊飯器などの家電がPLC (Power Line Communication) 網や無線LAN網を通じてネットワーク化されている。さらに、V2H (Vehicle to Home) という言葉に代表されるように両者が情報系ネットワークを通じてだけでなくエネルギー面でも連携しつつある。

このような民生品だけでなく、電力、ガス、上下水道、交通網、通信網などの重要インフラもマイコン化、ネットワーク化が進行している。もちろん、それは家電や自動車とも連携を深めている。全部を一まとめにするIoT (Internet of Things) とビッグデータという言葉が喧しい。

正に技術屋の本懐。小さなマイコンチップに見た夢が大きく広がり、世界を覆っている。私は、その広がり

深く関わってきた。今、「満足か？」と問われると「否」と答えざるを得ない。実は、二つの債務が残っている。この清算無くして満足とはいえない。

債務の一つはブラックボックス化というマイコン化に伴う弊害である。自動車部品のマイコンで数十万行のソフトウェア、スマホで数千万行。パソコンは一億行のソフトウェアが搭載されている。A4用紙一枚40行弱。100枚あれば単行本ができる。まけて、単行本一冊5千行とすると、自動車部品で単行本百冊、スマホで千冊、パソコンで一万冊に相当する。百冊は本棚、千冊は書庫、一万冊は図書館である。これは人の理解を越えている。

一般の方々はスマホを表面的には使えるだろう。しかし、内部がどのように動き、スマホが何所と通信をしているか把握できていない。実は一般の方々だけでなく、プロも把握できていない。専門家と言っても人間、頑張って一時に単行本十冊程度が理解の限界である。本棚も、書庫も、図書館も人知を越える情報量である。

もっとも、これはソフトウェアだけの話である。それにメカ部品や電子部品が連動している。もはや、作る側も使う側も理解できないマイコン化製品に人々は囲まれている。それが現代人の日常であり、大きな問題である。

この問題の解決にはメカ部品、電子部品、ソフトウェアなどを統合的に扱うフレームワークが必須である。そこで、電気通信大学では横河電機(株)の力も借りて、2006年から大学院学生を対象に高度IT人材養成コースを運営している。このコースでは制御系設計CADを用いて各部品をグラフィカルな表現の下、連携させてシミュレーションをしながら設計していく実践教育を行っている。加えて、オープンラボや高校などへの出張講義を通して広く一般の方々にマイコン化、ネットワーク化の本質を啓蒙している。

もう一つの債務がサイバーセキュリティ問題である。善人ばかりのユートピア。そんな桃源郷は存在しない。存在すると譲ってみても、そんな場所は脆弱性の塊である。悪人にとり、善人の集合ほど美味しい場所は無い。

世の中は善人も悪人もいる。ネットワーク化は便利な

反面、危険である。パソコンでは何らかのセキュリティソフトを使うのが常識である。情報システムにファイアーウォールは必須である。今、制御機器もネットワーク機器化し、セキュリティ対策が要望されている。

このような対策が常識化する以前の2010年にはイランのナタンのウラン濃縮工場がサイバー攻撃を受けた。そして、2011年3月11日の東日本大震災では被災地の重要インフラが壊滅した。使えるのが当たり前の電気、ガス、水道が停止した。時間通り来るはずの電車が破壊され、つながるはずの携帯電話が役に立たなくなった。被害は被災地に留まらなかった。東京電力管内では計画停電が行われた。現在でも、原子力発電停止による電力不足とエネルギー代金の高騰に日本中が悩まされている。

この2010年と2011年の出来事を受けて2012年3月に経済産業省の技術研究組合という枠組みでCSSC（制御システムセキュリティセンター）が発足した。横河電機（株）も初期メンバーであり、このような問題が起きる前から制御機器のサイバーセキュリティ対策を進めていた。また、計測自動制御学会では、2004年から産業応用部門でサイバーセキュリティ問題に取り組んできた。この活動は日本電気計測器工業会、JPCERT/CCとも協力して、この分野の重要性の啓蒙と対策の普及に取り組んできた。このような下地があったことがCSSCの敏速な設立につながった。

2013年5月には被災地の宮城県多賀城市のソニー工場跡の宮城復興パーク内に東北多賀城本部を設置し、サイバーセキュリティ対策の啓蒙や研究に使う模擬プラント7基をお披露目した。

制御システムは電力やガス、水道など使われる業種によって異なる。また、実際に稼働している装置を用いて研究開発を行うことができない。このため、模擬プラントが必須である。もっとも、重要インフラを広くカバーする7基もの模擬プラントを持っているのは世界に例がない。このため、お披露目後は国内、国外からサイバーセキュリティに関心を持つ要人が多数視察に訪れて頂いた。

2013年度の活動で特筆すべきことは認証業務の開始である。これも経済産業省の支援を受けた。一つはEDSA (Embedded Device Security Assessment) 認証であり、CSSCは2014年7月に横河のCENTUM VPと日立

のHISEC 04/R900Eを認証した。もっとも、横河は同年1月にProSafe-RSで同様の認証を米国のISCIEから得ている。この知見はCSSCの認証事業に活かされているし、CSSCもISCIEと連携して事業を進めている。

もう一つの認証事業としてJIPDEC（日本情報経済社会推進協会）が進めているCSMS (Cyber Security Management System)がある。これは、国内で4000社以上が認証を受けているISMS (information Security Management System)を下に、センサやアクチュエータを含む制御システムにセキュリティ管理を広げたものである。これの予備認証を2014年4月に横河ソリューションサービス（株）と三菱化学エンジニアリング（株）に与えた。これは世界で初めての認証である。このCSMS認証もCSSCがサポートしている。

時代は第三者認証である。自分で自分の製品の良さを主張することが第一人者認証。これはお手盛り。発注先が納品時に検査するのが第二者。これは広く行われているが、納品先ごとに基準が違う。そこで、利害関係がない第三者機関が統一基準で行うものが第三者認証である。これで認証の独立性が保たれるだけでなく、一度の認証で多くの発注先に納品できる。また、発注側も統一された基準の商品を広く集めることができる。

20世紀は大量生産の時代であった。物が無かったから、低コストで大量に作る必要があった。しかし、成長した21世紀の社会は安全、安心と個別化が求められている。前の二つは第三者認証が提供する。そして、提供された安全、安心のプラットフォーム上で、個々の要求を短納期で実現する製品や生産方式が求められている。CSSCはプラットフォームを作り、国内、国外の皆様に安全、安心を提供していきたい。そして、その上で、さらなる利便性を各組企業には実現して欲しい。

以上、これまでの私の研究者、技術者としての人生はわくわく感に溢れたものであった。残った二つの債務の解消は課せられた役務だと認識している。故井上ひさし氏の言「難しいことを易しく、易しいことを深く、深いことを面白く」を踏まえて、ネットワーク化されたマイコン機器の仕組みを啓蒙していくとともに、サイバーセキュリティ対策を進めていきたい。