進化する制御システムの先にある未来とは

JNSA 理事
セコムトラストシステムズ株式会社
藤川　春久

1997年5月、テルアビブにある某社でVPN製品の技術研修を受けていました。ようやく標準化が進んだIPsecベースの製品で、高額な専用線からインターネットを利用した仮想専用線の時代になるとかで、いち早くビジネスで活用すべく研修に参加していました。私のサイバーセキュリティとの関わりはここから始まったように思います。その後、19年近くサイバーセキュリティに携わってきた中で常に感じていた事は、見えない脅威から守るばかりで能動的に脅威と対峙できないというジレンマ。IoTが進行する現在ではあらゆる製品に搭載されているシステムの中身が分からないことから生じる不安も感じざるを得ません。

昨年、ドイツ車で排気ガスの不正が発覚しました。不正は「違法なソフトウェア」によるもので、リコールはソフトウェアの修正が中心になるということでした。車に搭載されている制御システム（ソフトウェア）は何ができるのか気になりました。最近の自動車は輸出先の国の法律や安全基準に適合するよう、車に搭載するコンピューター（以下、車載システム）が非常に細かく制御できるようになっており、エンジンの制御だけでなく走行機能や電子機器など車全体を制御できるようです。もしも、この車載システムに誰でもアクセスでき、重要な制御機能の設定が変更されてしまったら、事故にも繋がりかねません。自動車を所有する個人が車載システムの設定情報を変更する方法（「Coding」と呼ばれている）について情報発信しているサイトがあることを知りました。私も車を所有しておりますが、点検等はディーラーにお任せしています。ディーラーによれば車の整備にはメーカー公認資格が必要で、専用システムが無ければ車載システムにアクセスできないとのこと。しかし実際には、車載システムにアクセスするためのプログラムや、車とPCをOBDIIコネクタとLANケーブルで接続する方法、ランチャーを起動すると車に接続を開始して車台番号が表示される等の情報がサイトに掲載されています。プログラムにはPINコード生成機能があり、認証手続き無しに車載システムにアクセスできるようです。OBDIIコネクタとWi-Fi機器が合体した製品もあるようで、これを利用すると車外からも設定変更が可能となるようです。メーカーがセキュリティ対策を強化する筈なので、この状態がこのまま続くとは思えませんが現時点ではアクセス制御の強化が必要な製品もあるようです。

自動車だけでなく身の回りの多くの製品がネットワーク接続できるようになりその先にはインターネットへの接点もある筈です。生活全体がインターネットと切り離せない社会の到来。安心した生活を送るにはサイバーセキュリティの更なる進化も必要な時代となってきたようです。