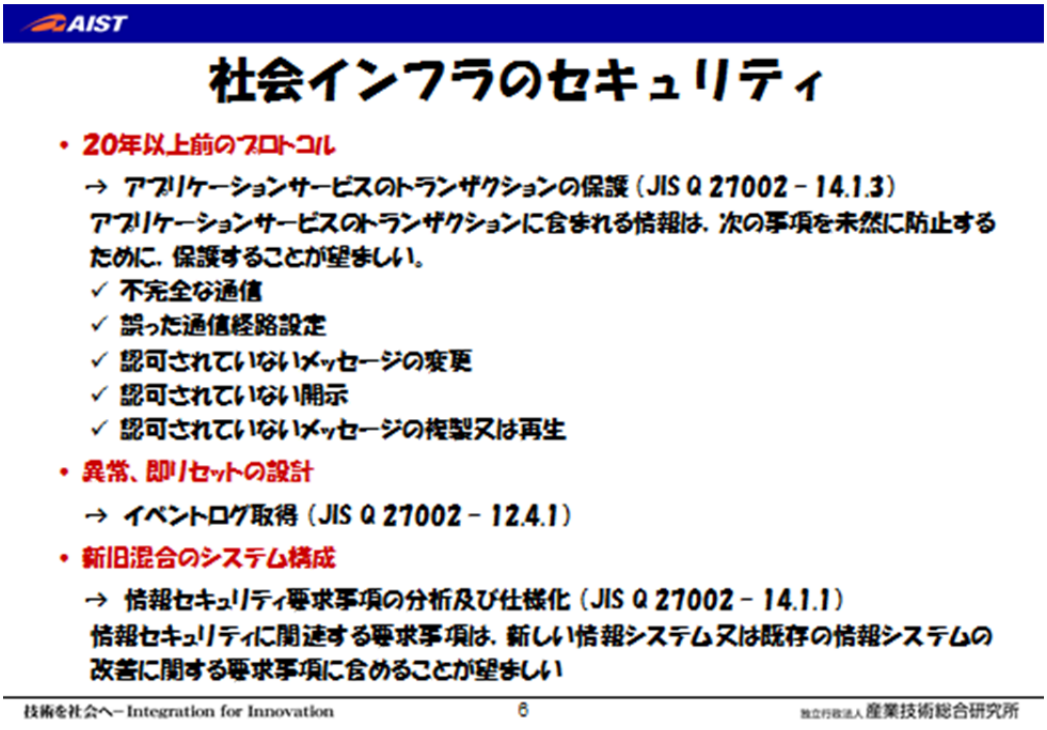
IoT 時代の組込みセキュリティ

国立研究開発法人　産業技術総合研究所
情報・人間工学領域　情報技術研究部門
サイバーフィジカル・セキュリティ研究グループ長
大崎　人士　氏

ここに一つのショッキングな動画がある。ビルの管理者でも何でもない一人の男性が、アムステルダムにある高層ビル 2 棟の電気を、スマートフォンを使って一瞬で消して見せている。これは、20 年以上前の設計思想で作ったプロトコルが使われていたり、組込み機器の最優先事項が動作し続けることにより異常が発生するとリセット、再稼働しログが残らない、といった設計の弱点が利用されている。また、新しいものを次々と入れるために、古いものが残ったまま全体を維持し続けなければならないという、新旧混合系システムの泣き所を示している。



■日本のセキュリティ制度

日本のセキュリティ制度はさまざまな点で 1995 年に英国規格協会（BSI）が作った BS 7799:1995 を基にしているが、それ以前はセキュリティをそれほど体系立てて考えていなかった。にもかかわらず、現在あらゆるところで使われているプロトコルはそれ以前のものである。さきほどの動画にあったビルは X10 という 1975 年に開発されたプロトコルを使

っており、日本でビル制御用プロトコルとして普及している BACnet が ANSI/ASHRAE135 として初めて規格化されたのは 1995 年、車載ネットワーク用に CAN が開発されたのは 1985 年である。昔の規格を使い続けつつ、守るべきものを守らなければならないという問題に現在、多くの製造業者が直面している。

「JIS Q 27002 情報技術ーセキュリティ技術ー情報セキュリティ管理策」はよくできている。JIS Q 27002-14.1.3 は、アプリケーションサービスのトランザクションを保護するように、JIS Q 27002-12.4.1 では、異常原因をたどれるようイベントログの取得を、JIS Q 27002-12.4.1 では情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含めることが望ましいと規定している。しかし、モノ作りの現場にはこれらの規定を完全に履行する余裕があまりない。

■セキュリティとセーフティのバランスを図るには

セキュリティとセーフティを混同して考えている人が少なくないが、私は常日頃セーフティとはクオリティ（品質特性）、セキュリティというのは活動であり、どう維持するかがセキュリティだと言っている。

安全分析の 1 つであるハザード分析では、被害の大きさと発生確率を乗じて算出するが、セキュリティ分析におけるリスク評価は脅威と脆弱性とパラメータという要素を考慮するもので、どういう弱点があるか、どういう攻撃を受けるかというリスクを考慮する際に、確率という要素は含まれない。

セキュリティとセーフティを両立するのは容易ではない。たとえばビルの出入り口を 1 つにすれば、侵入者の監視は容易になるが、非常時の避難路としては問題である。干渉しあうセキュリティとセーフティをどのようにシステム全体に取り入れていくかが悩ましい点である。

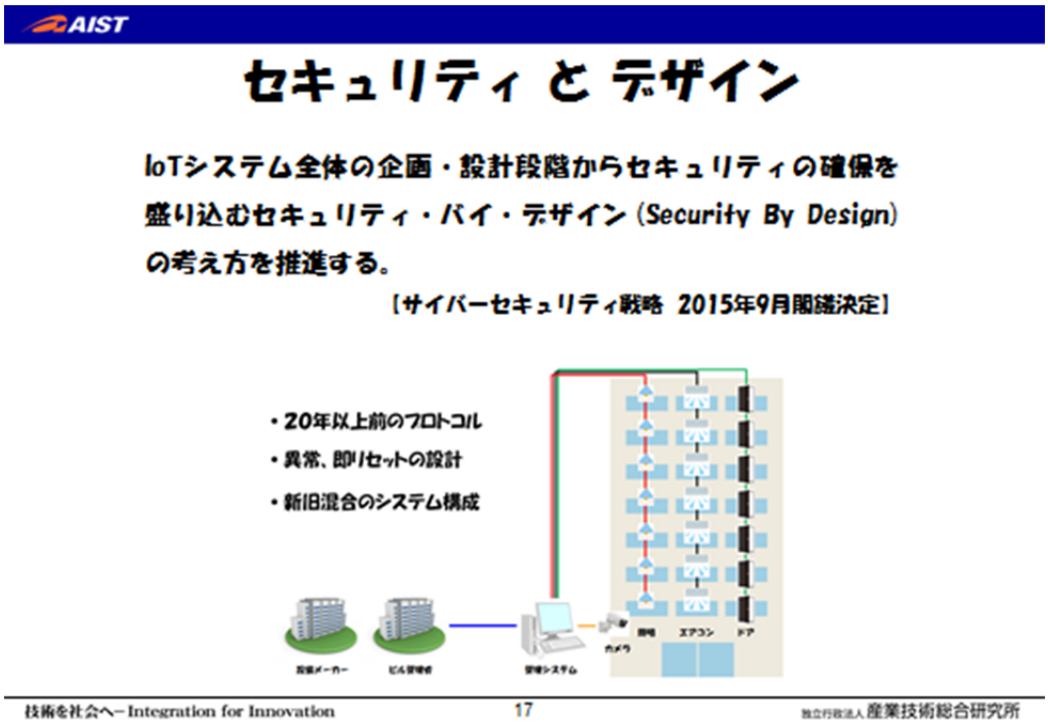
しかし一方、安全性テストの 1 つである異常注入テスト（fault injection）はセキュリティテストにおけるファジングと類似しており、セーフティとセキュリティで類似している点も少なくない。セーフティとセキュリティのバランスを図るには、双方の視点を持ち、互いの意図や考え方を理解し、伝え方を持つことが重要であろう。

■Security By Design

繰り返しになるが、セキュリティとは維持するための活動なので、無理があると続かない。今後製造業者は、セキュリティをデザイン（Security By Design）としてどう取り込んでいくかを考えていくことが重要であろう。

しかし、開発現場では要件定義から機能実装に至るまで要件定義書の作成から設計など膨大な作業を行っており、さらにセキュリティ要件分析を行おうとすると、大変な手間がかかる。そこで産総研では大量の要件の分析にかかる手間を自動化し、結果を可視化し、他ツールと連携するセキュリティ要求分析ツールを開発した。こうしたツールを活用すれ

ば製造業におけるセキュリティ対策に係る負担も大幅に軽減され、セキュリティ対策に積極的に取り組む事業者も多くなると思われる。



■組込み特有の問題解決に向けて

マイコンは暴走するものだ。暴走原因は不明であることが大半だが、ノイズで CPU がおかしくなることがほとんどである。そのため通常マイコンにはウォッチドッグタイマーがあり、異常時にはリセットするようになっている。しかしながら、この安全機能が正常に働かなかったために大事故もたびたび発生している。

そこで産総研では、異常停止しにくくするマイクロリセットマイコンを開発した。ノイズを 1 実験あたり 1 万回（0.25 秒毎）発生させるという過酷な実験に対して、異常（暴走）状態からの回復率が 95%という、自然界で使っている限りはまず暴走が起きないレベルまでに達した。

こうした強い耐性を持ったマイコンは、海底、高所といった人が関与できない場所の装置や、医療機器など即停止や即リセットが危険な装置、また、バッテリ式センサーなど、数が多すぎて人手をかける限界のある装置への適用が可能であろう。

今後、IoT 社会の実現に伴い、ますます多くの場面にマイコンが組み込まれていくだろう。こうしたリセットマイコンの普及は、より安心な社会の到来に寄与すると考えている。