ソフトウェア高信頼性とサイバーセキュリティ

技術研究組合制御システムセキュリティセンター（CSSC）理事長
国立大学法人電気通信大学情報理工学研究科 教授
新　誠一

現在、社会にサービスを提供している組込み系ソフトウェアのサイバーセキュリティ関連の活動を紹介する。合わせて、SEC が中心となって進めているソフトウェアの高信頼性手法をサイバーセキュリティ確保へ適用していくことを提案する。

2010 年夏に出現した stuxnet はイランの核燃料施設を攻撃した。このことが大きな転機となって、制御系のサイバーセキュリティ問題への取り組みが本格化した。制御システムセキュリティセンター（CSSC）は、2011 年 3 月に経済産業省の技術研究組合という形で民間企業を中心として発足した。IPA には組合員として当初から貢献頂いている。この場を借りて御礼申し上げる。

2012 年 7 月にお台場にある産業総合研究所内に東京研究センター（TRC）を設置し、2013 年 4 月には被災地である宮城県多賀城市に東北多賀城本部（TTHQ）を設置した。ここには国の補助を受け 7 台のテストベッドを研究、啓蒙、訓練、演習、標準化、認証などの業務を行うために作成した。TTHQ のお披露目を 2013 年 5 月に行って以来、国内外から多数の見学者に訪れて頂いている。詳しくは、本特集中の当組合の小林専務理事の解説を参照願いたい。

本稿では題目に従い、ソフトウェア高信頼性とサイバーセキュリティの問題を論じたい。まず、制御にソフトウェアをなぜ用いる必要があるかという根源的な問いについてであるが、それは「便利」だからである。容易にアルゴリズムや制御装置内のパラメータを変更できるので、時代、季節、個人などの状況に合った制御を行える。それ以上に、開発段階で何度も手直しが出来る。その意味では、「ソフト」である便利さとサイバーセキュリティの脆弱性は裏腹の関係である。

もちろん、ソフトの改変には認証などのセキュリティ機能が搭載されているものもある。しかしながら、国会や官庁、有力企業のサーバーから情報が引き出されている現状を鑑みると、現状のセキュリティ対策だけに頼るのは危険である。しかも、制御系は情報ネットワークだけでなく、制御ネットワーク、デバイスネットワークと攻撃される場所が多様である。制御システムセキュリティを確保するには情報セキュリティ技術と制御システム技術と両方に精通している必要がある。もっとも、片方の技術を習得するだけでも困難なのに、両方習得は無理である。そこで、連携が不可欠である。

この連携という視点で見ると、ソフトウェア高信頼性技術とサイバーセキュリティ技術は関係が深い。セキュリティが脆弱であれば、高信頼性とは言えない。また、逆に高信頼性のために磨いてきた手法がサイバーセキュリティにも有効である。例えば、相互レビューや相互依存性解析などの手法には注目している。

その中でも、HAZOP 解析 [1][2] は制御系セキュリティと関係が深い。この解析は、もともと化学工業における安全性確保で生まれたものである。これをソフトウェアに適用することで操作ミスや故障に強いソフトウェア、すなわち高信頼性を担保している。

制御系においても、すべてにセキュリティ対策をすることは難しい。システムの機能レベルを分析して、コストを懸けるべき所を洗い出す必要がある。その意味で、セキュリティ要件を HAZOP に入れていくことが高信頼性と高セキュリティを両立させる早道だと思う。

もちろん、相互レビューも FTA や FMEA、単体試験に統合試験などの各種高信頼性技術も有効である。サイバーセキュリティ対策も含めて、SEC でソフトウェアの高信頼性を研究開発して頂ければ幸いである。

【参考文献】
[1] http://www.ipa.go.jp/files/000005325.pdf
[2] http://www.ipa.go.jp/files/000004108.pdf