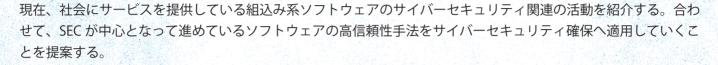
ソフトウェア高信頼性と サイバーセキュリティ

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



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