2J-03

計量機器のリモート更新機能実装に向けた関連法規制と国際規格に対するソフトウェア要件の提案

関本　泰之†　　後藤　厚宏†

情報セキュリティ大学院大学†

1. はじめに

機器メーカーにおいて、販売後の機器に対するメンテナンスは多くの時間とコストを要す。特にガソリンスタンドの給油機のように広く分散配置され、社会インフラの一部として活用されている機器については、メンテナンスのために設置場所に訪問することにより移動時間や交通費などがかさむ原因となる。そこでソフトウェア設計の観点から、メンテナンス上の課題を解決すべくリモート更新可能なシステム構築を目指し、その際に必要となるソフトウェア要件について提案する。

2. 対象機器と研究方針

本研究では対象機器を自動車等に燃料を供給するためのガソリン給油機（水以外の液体を対象とする特定計量機器：自動計量機器）とした。対象機器を「計量機器」と限定したことによって、ネットワークに接続される機器（いわゆる IoT 機器）の側面と、商取引に使用される社会的に重要な機器である側面を併せ持つ。つまり、該当分野の法規制やセキュリティなどを遵守しつつ、業務効率化を目指したソフトウェアのリモート更新を実現させることは、パソコンのようなリモート更新が前提の機器とは性質が異なり、そのソフトウェア要件は未解決な部分が多いことから、本研究の成果は社会的貢献度も高い。この計量機器のリモート更新機能の実装に必要な要件リストを作成するため、①関連する法規制・国際規格、②機器のシステム上の要件（セキュリティ）、③実運用上の要件の 3 つの要件について取りまとめをおこない、実用的なシステム構築に必要なソフトウェア要件を提案する。

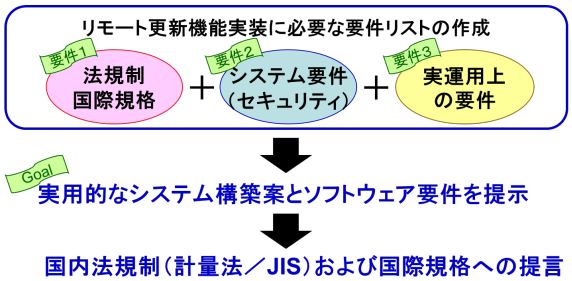

図 1　研究方針

Proposal of remote updating function software requirements in specified measuring instruments for related regulations and international standards
†Yasuyuki SEKIMOTO, Atsuhiro GOTO
†Institute of Information Security

3. 必要要件リストの作成

3.1 脅威分析

機器に対する脅威分析をおこなうため、まずは攻撃をパターン別に分類した。パターン分類としては、ネットワーク接続を経由した「外部通信」による攻撃、機器本体のハードウェアに対する「物理的な破壊・改ざん」による攻撃、送受信されるデータと内部データを対象とした「受信および内部データの改ざん」による攻撃、機器本来の機能を悪用した「不正操作」による攻撃が挙げられる。以下に各パターン別の脅威分析結果を提示する。

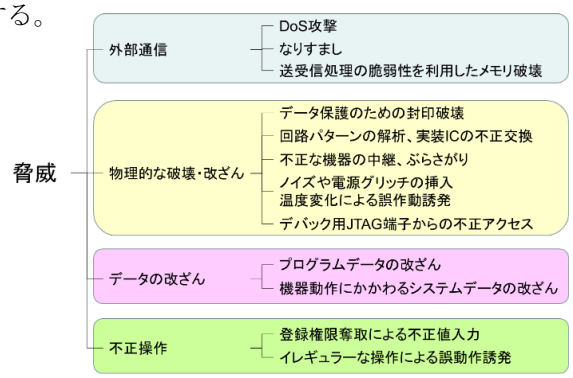

図 2　パターン別脅威分析

3.2 実運用上の必要要件

現在のメンテナンスにおけるプログラム更新作業をリモート更新に置き換えて分析した。

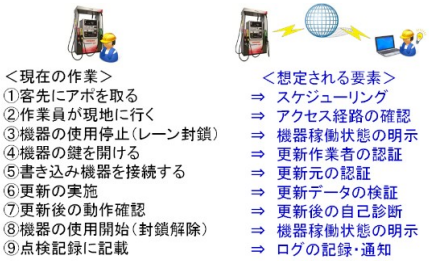

図 3　現在の作業と想定される要素

機能別分類として、リモート更新可能なシステムを構築するうえで事前に検討し仕様を確定する必要がある「システム構築の前提条件」、現在の作業をリモートに置き換えるうえで機器側に必要となる「機器側の追加機能」、作業が適正であることを確認するための「システム間の認証」に分類して分析した。

3.3 必要要件のまとめ

脅威分析と実運用上の要件について取りまとめをおこない要件リストを作成した。その際に、保護策が重複する項目については対象から除外した。

表１　必要となる要件リスト

脅威／運用	保護策／要件
「外部通信」による攻撃	
DoS攻撃	通信ポートの開閉制御
	通信制御処理による受信データ制限
なりすまし	データサーバの認証
	通信の暗号化
送受信処理の脆弱性を利用したメモリ破壊	送受信処理の対策強化
「物理的な破壊・改ざん」による攻撃	
データ保護のための封印破壊	電子封印システム
回路パターンの解析、実装ICの不正交換	基板のコーティング
	実装ICのSOP化
不正な機器の中継、ぶらさがり	機器間のデータチェック
	通信の暗号化
ノイズや電源グリッチの挿入、温度変化による誤作動誘発	ノイズ対策
	ソフトウェアによる誤動作防止の対策強化
デバック用JTAG端子からの不正アクセス	デバック用JATG端子のパターンおよび端子を削除
「受信および内部データの改ざん」による攻撃	
プログラムデータの改ざん	プログラムデータの信頼性確認
	データの完全性確認
	チェックサム
	アップデート・監査ログ
	Root of Trust／Chain of Trust
内部データの改ざん（機器動作にかかわるシステムデータ）	内部データのアクセス保護
	データの完全性確認
	チェックサム
	変更・監査ログ
	TSIP／Trust Zone
「不正操作」による攻撃	
登録権限の奪取による不正値入力（特に機器のコアデータ）	権限の厳格管理
	操作者の限定
	コアデータのアクセス保護
イレギュラーな操作による誤動作誘発	標準的な入出力に対する誤動作防止の対策強化
実運用上で求められる要件（不足分）	
システム構築の前提条件	スケジューリング
	アクセス経路の選択
機器側の追加機能	機器稼働状態の明示
システム間の認証	更新作業者の認証（データサーバ側の権限）

4. 計量機器をとりまく法規制と国際規格

国内においては「計量法／JIS」が挙げられるが、ソフトウェアに関する項目およびセキュリティ面での定義は少ない。そこで、JIS 規格のベースとなっている OIML（国際法定計量機関:International Organization of Legal Metrology）が定める要件、および欧州規格である WELMEC 文書からソフトウェアに関する計量規格を調査した。対象としては、国内の JIS 規格の中でもソフトウェア要件が具体的に含まれている「JIS B 7611-2」[1]、OIML が発行する国際文書のうちソフトウェアに関する統一された指針や参考情報を与える文書である「OIML D31(2008)」[2]、欧州規格で非自動計量機器を対象とした「WELMEC 2.3」[3]、WELMEC 2.3[3]から分化し自動計量機器を対象とした「WELMEC 7.2」[4]のソフトウェア要件について調査した。

5. 脅威に対する保護策の考察と追加要件の検討

脅威分析および実運用上の必要要件から作成した要件リストと、調査した各法規制で対象となっている要件を比較し、該当するソフトウェア要件がない部分が不足分であると仮定することできる。外部通信に対する保護策として接続先を確認するための「データサーバの認証」、物理的な破壊・改ざんに対する保護策としてハードウェアパターンを保護するための「ハードウェア保護（JTAG 端子ほか）」、内部データの改ざんに対する保護策としてプログラム起動からの信頼性確認をおこなう「ブートプロセス（セキュアブート）」およびセキュア IC に代表されるような「メモリ保護（セキュア IC）」、不正操作に対する保護策としてコアデータへのアクセス制限のための「コアデータのアクセス保護」、最後に実運用上の要件として「スケジューリング」および「機器稼働状態の明示」の全 7 項目について、不足分を補うための追加要件とした。

6. ソフトウェア要件リストの作成

前項で検討した追加要件も含め、実用的なシステム構築に必要なソフトウェア要件リストを作成した。リストの作成においては、調査対象とした各法規制をベースにソフトウェア要件を参照し、不足している追加要件部分については追記する形式で作成した。研究の対象機器に該当しない非自動計量機器に対する要件である JIS B 7611-2[1]や WELMEC 2.3[3]も参照先に含めることで幅広い脅威から保護可能なソフトウェア要件となった。

表２　ソフトウェア要件リストの構成

1. 一般要件
- 1．1 ソフトウェア識別
- 1．2 アルゴリズムと機能の正しさ
- 1．3 ソフトウェア保護
  - 1．3．1 誤操作防止
  - 1．3．2 メモリ保護
  - 1．3．3 固有パラメータの保護
  - 1．3．4 封印によるソフトウェア保護
  - 1．3．5 ブートプロセス（セキュアブート）
- 1．4 ユーザーインタフェース
  - 1．4．1 コアデータのアクセス保護
- 1．5 ハードウェア機能の支援
  - 1．5．1 故障の検出
  - 1．5．2 耐久性の検出
  - 1．5．3 ハードウェア保護（JTAG端子ほか）
- 1．6 測定データの提示

2. 機能別要件
- 2．1 ソフトウェアの分離
  - 2．1．1 電子装置の部品装置の分離
  - 2．1．2 ソフトウェア部分の分離
- 2．2 表示の共有
- 2．3 ソフトウェアダウンロード
  - 2．3．1 法定計量ソフトウェア
  - 2．3．2 ソフトウェア更新
    - 2．3．2．1 立ち合い者あり
    - 2．3．2．2 立ち合い者なし
      - ① スケジューリング
      - ② 機器稼働状態の明示
  - 2．3．3 装置固有パラメータの設定
  - 2．3．4 法定計量に関連するソフトウェア範囲
  - 2．3．5 データサーバーの認証
- 2．4 データの保存
  - 2．4．1 保存すべき情報
  - 2．4．2 暗号化
  - 2．4．3 自動保存
  - 2．4．4 時刻刻印
  - 2．4．5 外部要因からの保護
  - 2．4．6 記憶容量と持続性
  - 2．4．7 メモリ保護（セキュアIC）
- 2．5 外部インタフェース
  - 2．5．1 インタフェースの保護
  - 2．5．2 通信暗号化
  - 2．5．3 データの保証（信頼性、完全性）
  - 2．5．4 外部要因からの保護
  - 2．5．5 破損したデータの取り扱い

7. まとめ

本研究では計量機器のリモート更新実現の際の環境変化を中心に脅威分析をおこなうとともに、これまで要素として考慮されてこなかった実運用面での必要となるソフトウェア要件についても考察をおこなうことでソフトウェア要件リストをまとめた。本研究が現状では OIML に準拠することでカバーされている国内法規制（計量法／JIS）および国際規格に対してソフトウェア要件・認証の策定や改定をおこなう際の議論に貢献できることを期待したい。

参考文献

[1] 経済産業省, “JIS B7611-2：非自動はかり－性能要件及び試験方法－　第２部：取引又は証明,” https://kikakurui.com/b7/B7611-2-2015-01.html.
[2] OIML, “OIML D31: General requirements for software controlled measuring instruments,” https://unit.aist.go.jp/mcml/rg-mi/softcert/files/matsuoka-oimld31_2013.pdf.
[3] WELMEC, “WELMEC 2.3,” https://www.welmec.org/fileadmin/user_files/publications/2-3.pdf.
[4] WELMEC, “WELMEC 7.2,” https://www.welmec.org/fileadmin/user_files/publications/WG_07/Guides/WELMEC_Guide_7.2_Software_Guide_2018.pdf.