組み込みシステムにおける安全なリモートアップデートの考察

Consideration of secure remote update in embedded system

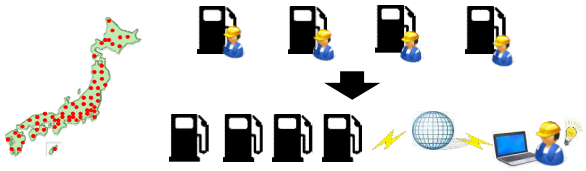
関本　泰之・マネジメント分科会・情報セキュリティ大学院大学

Abstract : In this research, I aim to present technical requirement for realizing Internet connection and remote update in embedded system with limited hardware resources. In this paper, I investigate the problem of connecting the equipment used locally to the Internet, the system requirements for secure remote update of the program, and the security requirements.

1．研究の背景と課題

1－1．リモートアップデートとは

フィールドに点在する機器・端末に対して遠隔地からプログラムや設定更新をおこなう技術。



1－2．現状の課題

機器はプログラムの更新をする必要性が生じる場合がある。

- ソフトウェアバグの修正
- 機能追加など

特にソフトウェアバグの修正においては顧客の信頼と機会損失に関わることから、迅速な対応が必要となるケースが多い。

1－3．研究対象とするシステム規模

機器によってシステムの規模が異なるため、必然的にプログラム領域やメモリ容量などハードウェアリソースに違いがある。

	OSなし	RTOS	汎用OS
代表例	–	ITRON VxWorks	Linux Android Windows
動作	シングルタスク	マルチタスク	マルチタスク
ハードウェア変更	小	小	大
システム価格	小	中	大

本研究では小・中規模システムをリモート化することへの提案と、そこにどのような脅威と課題が存在するかを考察する。

1－4．現状の課題を解決するための提案

次のようなシステムの達成を目指す。

“フィールドに点在する機器を、その稼働を妨げることなく、安全かつ確実にかつ自動的にプログラムアップデートを実行する”

リモートアップデートにより、設置場所に関わらず迅速な対応が可能になる。

例）日本国内に３０，０００カ所ある設置場所にプログラム更新をおこなう場合。

＜現在＞
作業人数　　：300人
作業量（一日）：2カ所
完了までの日数：50日

⇒

＜リモート化＞
作業人数　　：**1人**
作業量（一日）：30,000カ所
完了までの日数：**1日**

工数削減
作業の迅速化
適切な保守・運用

1－5．実運用上の要素

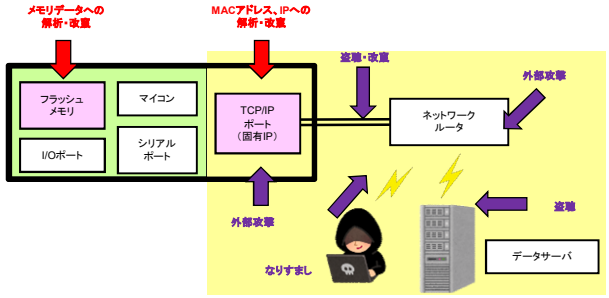
現在の作業をリモート化に置き換えた場合について考察する。

＜現在の作業＞		＜想定される要素＞
①客先にアポを取る	⇒	スケジューリング
②作業員が現地に行く	⇒	アクセス経路の確認
③機器の使用停止（レーン封鎖）	⇒	機器稼働状態の明示
④機器の鍵を開ける	⇒	更新作業者の認証
⑤書き込み機器を接続する	⇒	更新元の認証
⑥更新の実施	⇒	更新データの検証
⑦更新後の動作確認	⇒	更新後の自己診断
⑧機器の使用開始（封鎖解除）	⇒	機器稼働状態の明示
⑨点検記録に記載	⇒	ログの記録・通知

1－6．リモート化によって生じる脅威

リモートアップデートを実行するためにはシステム構成の変更、およびネットワーク接続が必要となる。

- システム構成の変更
  これまでマイコンのROM領域のみ保存されていたプログラムデータを実行中にダウンロードするための外部メモリが必要となる。
  追加となるハードウェアに対する攻撃を考慮しなければならない。
  ⇒セキュリティ課題：物理タンパ性、セキュア部の分離
- ネットワーク接続
  これまでローカルで使用されていた機器がネットワークに接続されることで脅威にさらされることを考慮しなければならない。
  ⇒セキュリティ課題：暗号通信、認証技術



2．関連技術の現状調査

異なる3つの観点から調査を実施し、考察をおこなった。

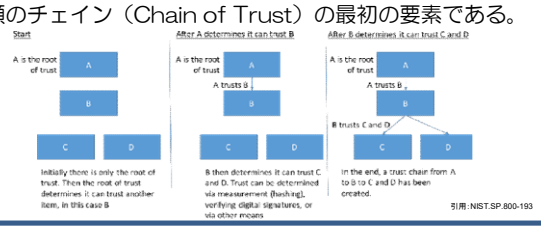
①リモートアップデート技術の運用事例
②セキュリティ保護に関するガイドライン
③リモートアップデートを実現するための機器構成

- セキュリティ原則

NIST SP800-193ガイドラインにおいて3つの項目を挙げている。
保護（Protection）・検出（Detection）・回復（Recovery）

- 信頼の起点：Root of Trust（RoT）

RoTはセキュリティ固有の機能を提供するための基礎を形成する要素。
RoTは信頼のチェイン（Chain of Trust）の最初の要素である。



3．今後の研究方針

- 技術課題の洗い出し
  Root of Trustによる信頼性の高いシステムを実現するため、組み込みシステム向けに提供されているセキュアICについて調査をおこない、実装に向けた技術課題について検討する。
- 信頼性を高める技術調査と技術課題の洗い出し
  ①ネットワーク接続される機器のセキュリティ要件の調査
  ②組み込み機器（小・中規模システム）におけるセキュリティ要件の組み込み制限についての考察
  ③システム規模別の推奨されるセキュリティ要件のリスト化
  ④実験を通じたセキュリティ要件リストの検証