

Promela における割り込み制御の半自動モデル化

フェリカネットワークス株式会社 只野 賢二 Kenji.Tadano@FeliCaNetworks.co.jp

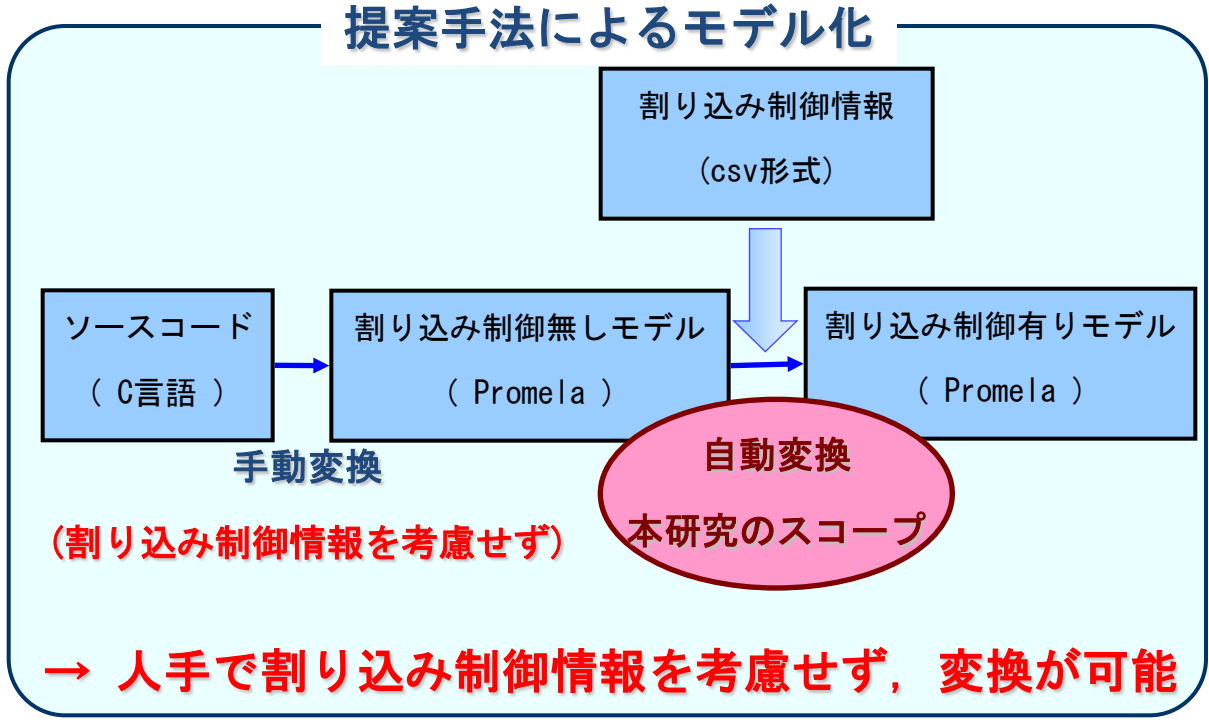
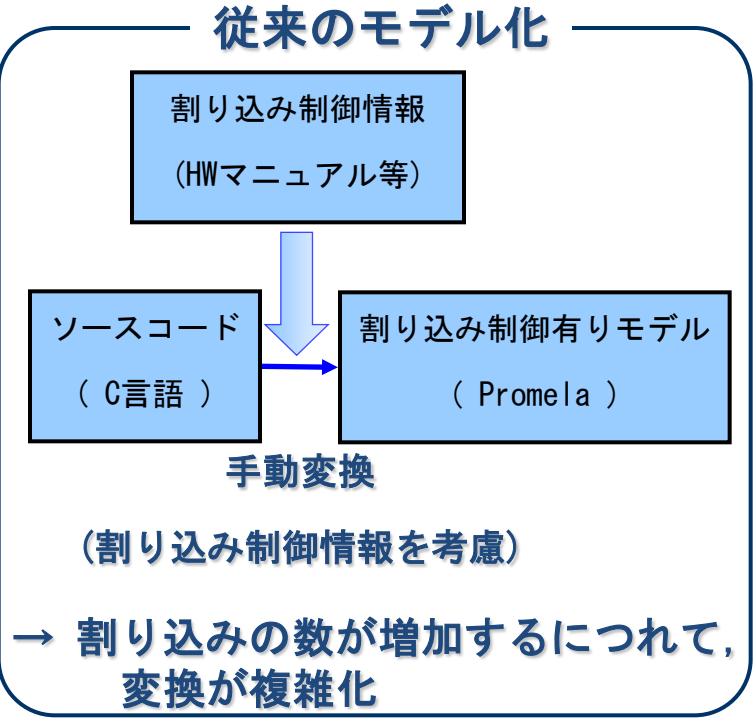
開発における課題

ファームウェアの品質向上手法として、モデル検査を導入するにあたり、C言語のソースコードをモデル記述言語である Promela に変換（モデル化）する必要がある。
 モデル化の過程で、割り込み制御情報をモデル化する必要があり、割り込みの数が増加するにつれて、モデル実装者の負担や実装中のミス混入が懸念される。

本研究の提案

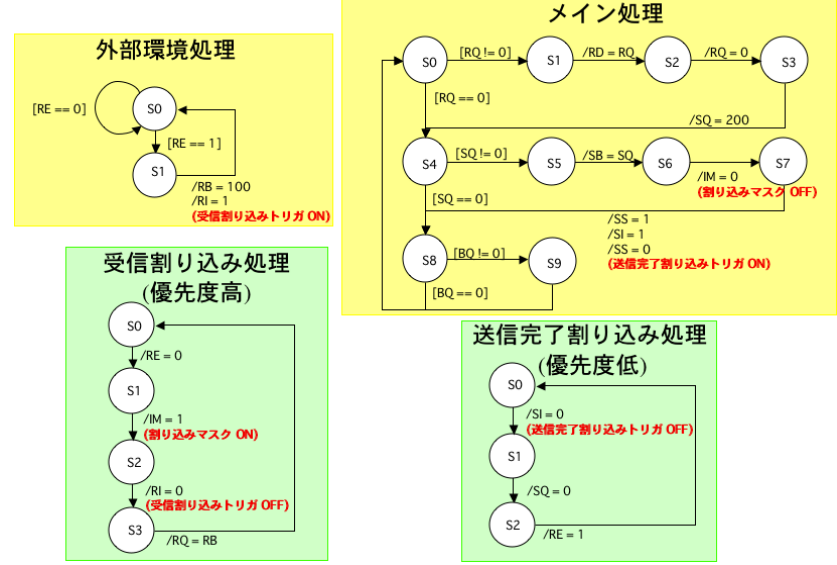
モデル実装者の負担軽減、実装中のミス混入軽減をするために、以下を機械的にモデル化する手法を提案する。
 ・多重割り込み
 ・割り込みマスク
 ※上記2つが割り込み制御情報のモデル化を複雑にする原因である。

研究の概略



実システムへの適応

モバイル FeliCa IC チップを本手法によりモデル化



→ 検証項目「いつか必ず RE == 1 となること」を確認

まとめ

本研究で行ったこと

- ・ 多重割り込み、割り込みマスクを考慮した割り込み制御情報を半自動でモデル化する手法を提案
- ・ 提案した手法を自動にて行う、変換ツールを作成し、ツールの妥当性を確認
- ・ 実システムへの適応による、有効性の確認

今後の展望

- ・ 規模のより大きいモデルへの適応
- ・ 複数割り込みが同時に動作する場合の考慮