トップエスイー修了制作

半順序を利用したカーネルドライバのデッドロック検出手法

株式会社クレスコ　聖城　豊　y-seijyo@cresco.co.jp

開発における問題点

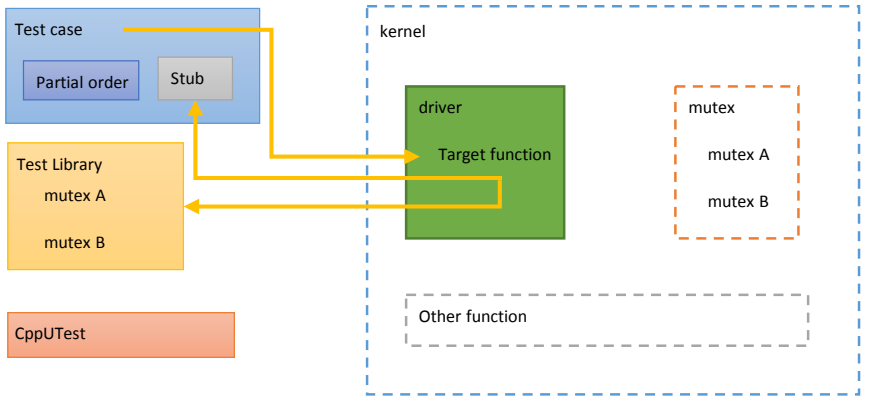
カーネルドライバの開発ではコア数の増大により，デッドロックが発生する可能性は高まっているがそれをテストする方法が定まっていないため，品質の確保が難しくなっている．静的解析や形式手法の利用は敷居が高く，コストの面などでも導入が難しい．

手法・ツールの提案による解決

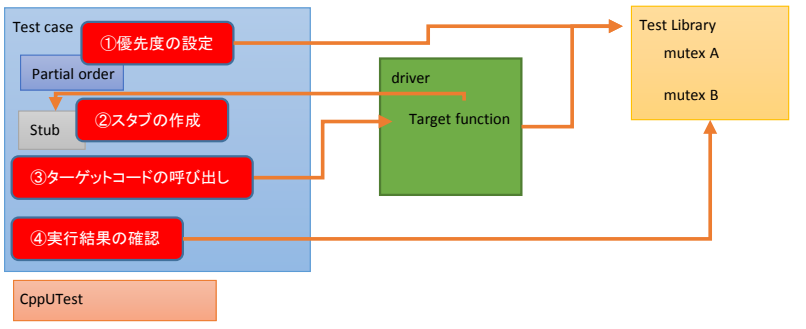
カーネルドライバのmutexデッドロックのテストに半順序を利用したテスト記述を導入することを提案する．
テスト記述を利用することにより，より実践的で開発者観点で受け入れやすいデッドロックの検出手法となっている．

mutexテストライブラリを利用した検出手法

mutexの優先度に半順序を設定し，mutex用に順序の設定，及び，利用順序のチェックを行うテストライブラリを作成した．これをmutexの処理を置き換えることにより，デッドロックの検出を行う．



テストケースは次のように作成を行う
1) 優先度に半順序を設定
2) スタブの作成
3) テストターゲットとなる関数の呼び出し
4) テストの実行結果の確認



他の手法との比較

手法	利点	欠点
静的解析	・ソースコードがあれば可能	・ツールを使うのにコストがかかる
モデル検査	・網羅的に検査できる	・モデルが必要となる ・関数ポインタを使う部分の検査が難しい
テスト記述	・開発者が理解しやすい ・柔軟な対応が可能	・必要となるスタブの数が多い ・ソースコードの理解が必要

まとめと今後の課題

現状，以下の課題がある．
- ドライバファイルやモジュール外の関数などにはすべてスタブが必要となってしまうため，手間がかかる．
- すべての処理が終わった後に結果の判定を行うため，検出した箇所がわかりづらい．

上記の課題に対して以下のような対策が考えられる
- スタブは自動生成し，必要な箇所のみ実装を加える
- 検出時に検出した箇所で実行をとめるようにする