平成23年度「通信プロトコルとその実装の安全性評価に関する研究開発（副題：「形式手法によるプロトコル実装の検証技術と形式仕様に基づく網羅的ブラックボックス検査技術の開発）」の研究開発目標・成果と今後の研究計画

1．実施機関・研究開発期間・研究開発費

◆実施機関　　独立行政法人産業技術総合研究所＜幹事＞、株式会社レピダム
◆研究開発期間　平成22年度から平成24年度（3年間）
◆研究開発費　　総額116百万円（平成23年度　35百万円）

2．研究開発の目標

本プロジェクトでは、形式的手法による通信プロトコルの規格の記述を元にその実装の様々な評価・検証手法を統一的に扱うことのできる手法および、ブラックボックスになっている実装においてもテストケースの網羅性などを保証し、仮想マシンモニタを利用した実行のトレース及びロールバックにより脆弱な実装を解析できる環境の開発を行う。

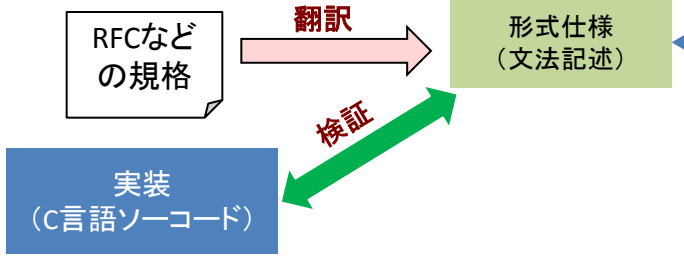
3．研究開発の成果

課題ア）「形式的手法によるプロトコル実装の検証技術の開発」と課題イ）「網羅的テストケース生成による実装のブラックボックス解析技術の開発」に分けて開発を行った

）

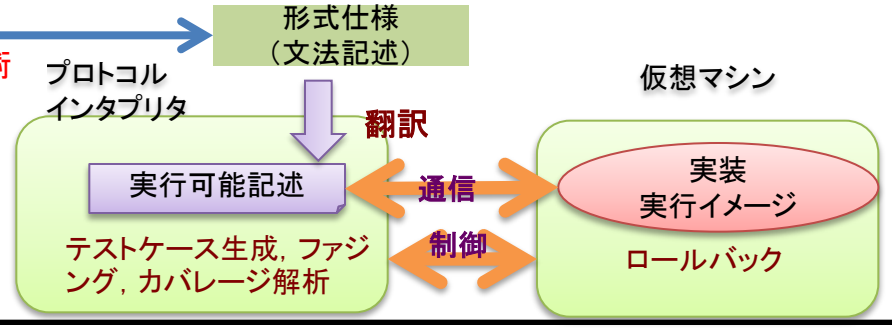
課題ア）形式的手法による プロトコル実装の検証技術の開発

通信プロトコルの安全ために形式的手法を用いて仕様とプログラムを検証する技術



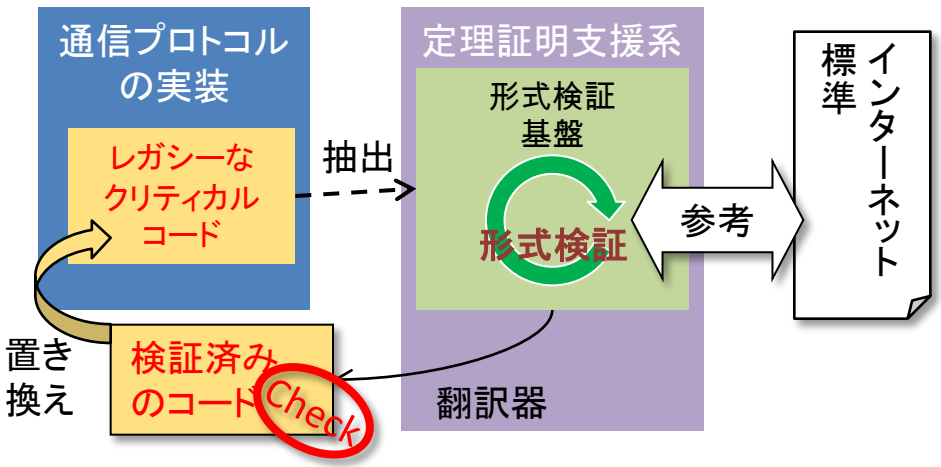
課題イ）網羅的テストケース生成による 実装のブラックボックス解析技術の開発

プログラムがブラックボックスであってもプロトコルの網羅的なテストケースによる検証とその実行を仮想マシンを用いて完全にトレースする技術を開発

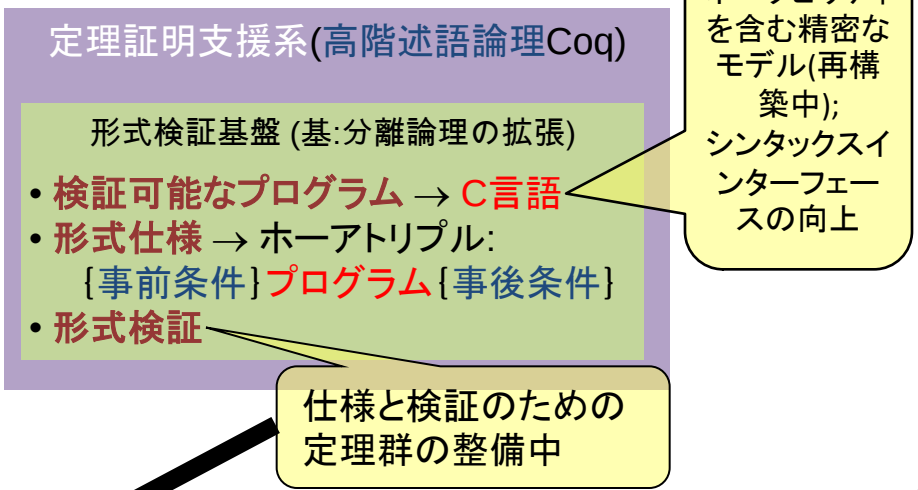


課題ア）形式的手法によるプロトコル実装の検証技術の開発の主な成果

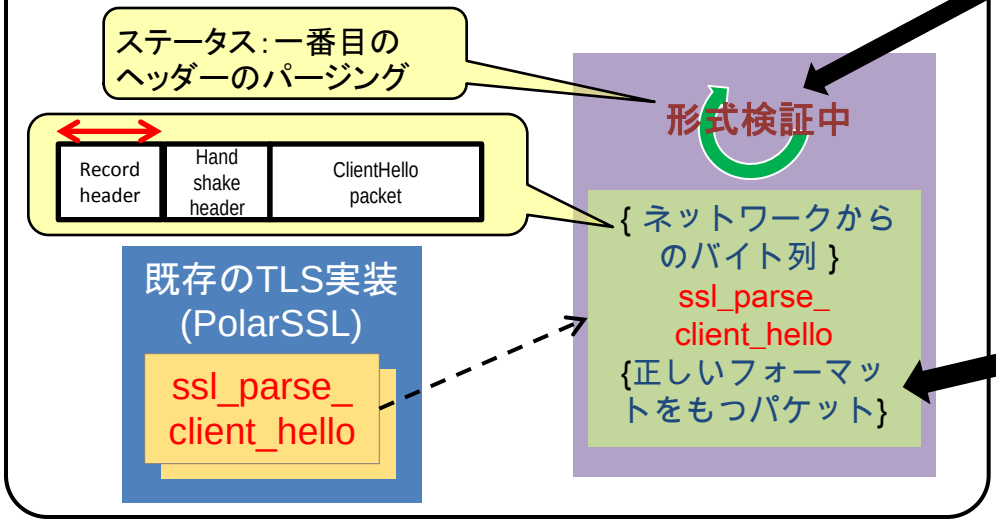
課題ア）形式的手法による プロトコル実装の検証技術の開発



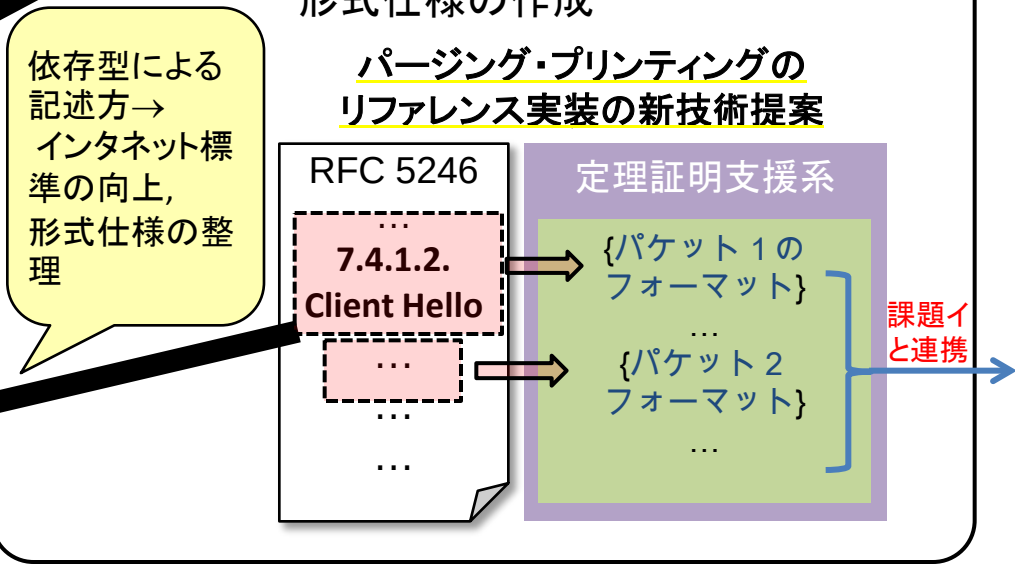
形式検証基盤



ケーススタディー作成



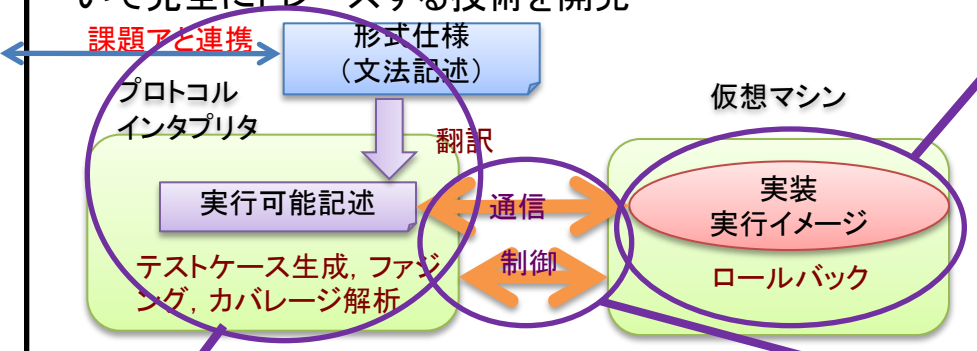
形式仕様の作成



課題イ）網羅的テストケース生成による実装のブラックボックス解析技術の開発の主な成果

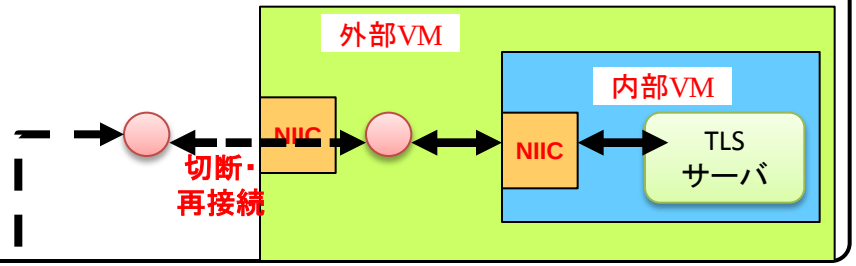
課題イ）網羅的テストケース生成による実装のブラックボックス解析技術の開発

プログラムがブラックボックスであってもプロトコルの網羅的なテストケースによる検証とその実行を仮想マシンを用いて完全にトレースする技術を開発



ネットワークの接続を保ったままロールバックする技術

ネットワークの接続を保持したままロールバックするために二重の仮想化技術とプロキシによって実現した。通常の仮想マシンのスナップショット機能ではネットワークの接続が保てないが、二重の仮想化とプロキシを使うことで内部VMのネットワークの接続は維持したままロールバックする。



プロトコル記述方式とリファレンス実装生成系

・プロトコル記述言語の仕様記述言語としての記述性・可読性と、リファレンス実装生成系としての表現力の両立が課題
→ 本年度は、主に仕様の可読性を中心に検討。昨年度の機能検討を元に新たな仕様記述言語を設計しプロトコルの一部を実際に新言語で記述した。
・今後、テスト生成との連携を踏まえた記述言語の詳細設計を進めるとともに、実際のテスト器の生成を処理計画超の形で行う

プロトコルテスト用通信制御モニタ通信手順

プロトコル検査にVMスナップショット・ロールバックを用いる際に、通信状態の同期を取り検査を正しく行うために、TCPストリームレベルの通信内容の伝送とVMの制御を一括して行う通信手順を定義した。これにより、課題イ－1）とイ－2）の間の連携を実現し、スナップショット・ロールバックを用いた網羅的検査の基盤を提供する。

プロトコルテスト用通信手順

- TCPレベルの通信の伝送（IP仮想化）
- 仮想機械の同期的巻き戻し操作
- 通信状態の監視・通知機能

4. これまで得られた成果（特許出願や論文発表等） ※成果数は累計件数と（ ）内の当該年度件数です。

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース	展示会	標準化提案
形式手法によるプロトコル実装の検証技術に関する研究開発	0	0	4{2}	0	0	0	0

5. 研究成果発表会等の開催について

（1）産学官連携のための所属組織の研究成果報告会を毎年主催し、All Japanの取り組みを牽引

情報セキュリティ研究センター 最終報告会
日時：平成24年3月23日（金）13:30-18:00 場所：秋葉原UDXビルUDXシアター
来賓挨拶経 済産業省 情報セキュリティ政策室
基調講演 東京電機大学教授（内閣官房情報セキュリティセンター情報セキュリティ補佐官 ）佐々木 良一教授

6. 今後の研究開発計画
この成果により、今後、どのような研究を行うのかを例示を上げながら、具体的、かつ簡潔に記載して下さい。

プロトコルの形式化とそれに基づく形式的・網羅的検査の手法を確立することにより、将来のプロトコルの検証およびテストの分野における発展に貢献する。今回の開発では通信プロトコルのパケット処理のソースコードの一部の形式検証ができるようにするが、今後、プロトコルの仕様から実装を直接的に形式検証ができるようにするために形式検証のライブラリの拡張する。また、形式仕様による網羅化と仮想化マシンモニタによる探索の効率化をベースとしたコントロールフロー解析については、形式仕様記述の更なる汎用化と適用範囲の拡大のほか、仮想計算機環境の拡充などによるルータなどのブラックボックス実装のようなより面倒な検査対象への技術の適用を計る。