平成22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）」の開発成果について

1. 施策の目標

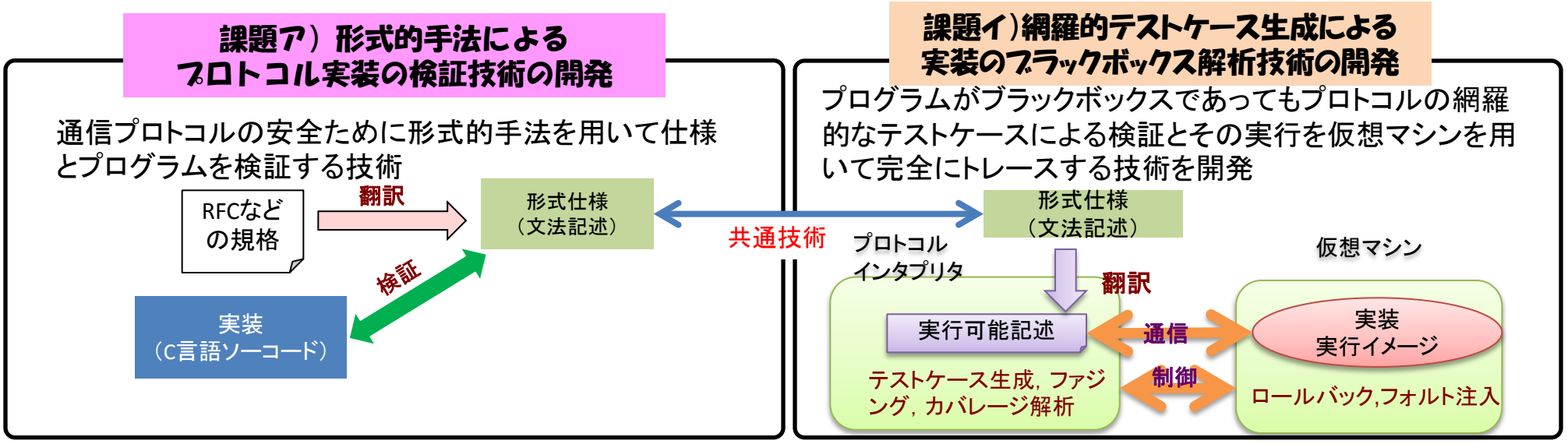
通信プロトコルの安全ために形式的手法を用いて仕様とプログラムを検証する技術、および実際のプログラムがブラックボックスであってもプロトコルの網羅的なテストケースによる検証とその実行を仮想マシンを用いて完全にトレースする技術を開発する。

2. 研究開発の背景

インターネット標準は現実の実装においては必ずしも仕様がその通りに反映されていない場合が多い。特に暗号通信プロトコルなどにおいて、その実装の誤りがセキュリティ上の脆弱性に繋がるケースが複数見受けられている。このような誤りはもちろん実装の作成者の注意不足に起因する場合も多いが、一方で誤りの一端が標準そのものにある場合もある。

3. 研究開発の概要と期待される効果

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。



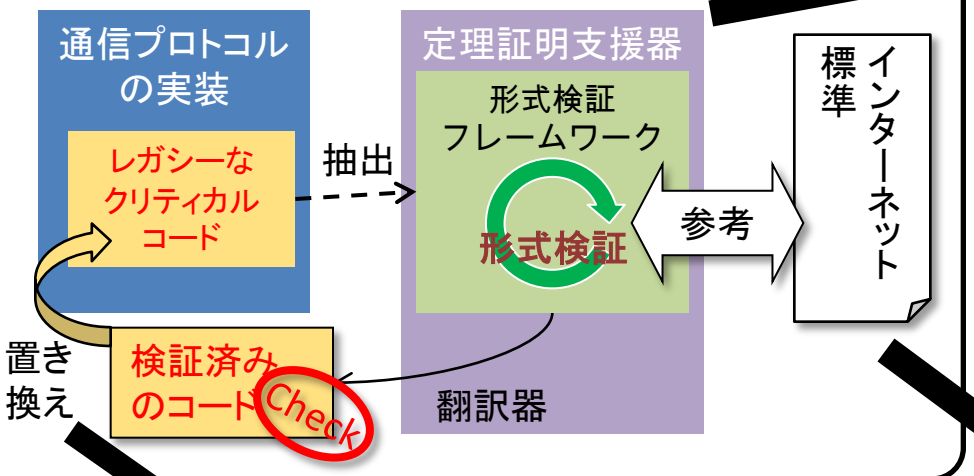
4. 研究開発の期間及び体制

平成22年度～平成24年度（3年間）

NICT委託研究（独立行政法人産業技術総合研究所、株式会社レピダム）

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



形式検証フレームワーク

定理証明支援器 → Coq（高階述語論理）

形式検証フレームワーク → 分離論理の拡張:

- 検証可能なプログラム → C言語
- 形式仕様 → ホーアトリプル:
  {事前条件}プログラム{事後条件}
- 形式検証 → ポインターを扱う証明系

翻訳器 → Cのモデルから実行可能なCへ

精密なモデル，型や演算子多数

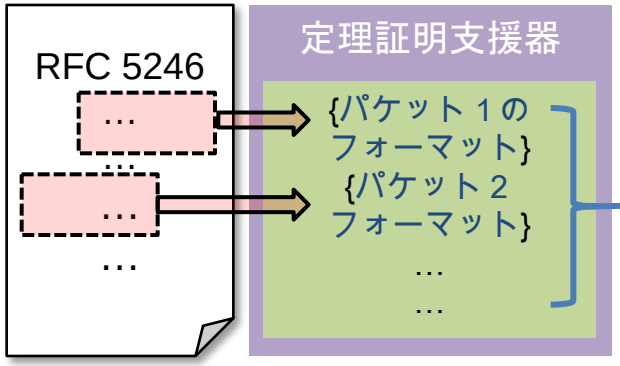
高階述語論理で高い表現力

動作確認済み

ケーススタディー作成

形式仕様の作成

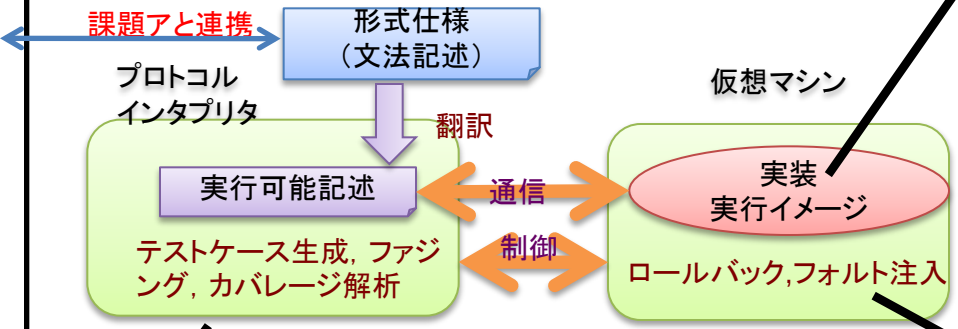
曖昧さのない記述へ向けて、定理証明支援器でRFCの形式化の依存型やモナドプログラミングによる技術は開発中



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

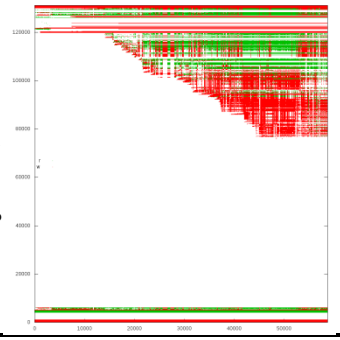
プログラムがブラックボックスであってもプロトコルの網羅的なテストケースによる検証とその実行を仮想マシンを用いて完全にトレースする技術を開発



仮想マシンから見た各プロセスのメモリトレース技術

CPUの持つ仮想記憶の仕組みを仮想マシン上で監視することで、OSに依存することなく各プロセスが物理メモリに割り当てている領域を監視できる技術を開発した。
具体的にはX86 CPUのCR3レジスタとページテーブルをトレースするソフトウェアを開発した。

左グラフは起動時からトレース。横軸が時間、縦軸がメモリ領域。青が読出し専用、赤が読書可。Linuxカーネルが物理メモリの下位を使い、ユーザプロセスが上位から使うことが分かる。



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、主に仕様を十分に実装できる表現力を中心に検討。プロトコルの一部を実際にCoqで実装し必要な言語機構を検討した。作成した部分は形式検証、リファレンス実装生成、さらに一般的なTLSプログラムとやり取り可能。
・今後、仕様としての可読性や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。

仮想マシンからブレークポイント技術

BlackHat USA 2010で発表した仮想マシンから任意の命令にブレークポイントを置く技術をプロトコルのプログラムトレースで利用できるか試験した。この技術はOSに依存せずにカーネルメモリ空間でもユーザメモリ空間でもブレークポイントを置くことができるが、プロジェクトで目指しているブラックボックスの実装に対する解析に適用するには、プロセスの構造自体を解析する必要があることが分かり、上記のプロセスメモリトレース技術と組み合わせて解析を行う必要があることを確認した。

1. これまで得られた研究成果（特許出願や論文発表等）

	国内出願	外国出願	研究論文	その他研究発表	報道発表	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	0	2	0	0	0

発表

1. アフェルト　レナルド、山田　聖、「分離論理を用いた, C言語プログラムの機械的検証」、13回プログラミングおよびプログラミング言語ワークショップ、日本ソフトウェア科学会、ポスター発表
2. David Nowak and Yutaka Oiwa, ”Specification-based verification and testing of Internet protocols”, 日本応用数理学会 (JSIAM), 「数理的技法による情報セキュリティ」研究部会 (FAIS)