平成24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＜幹事者＞、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24年度 36百万円）

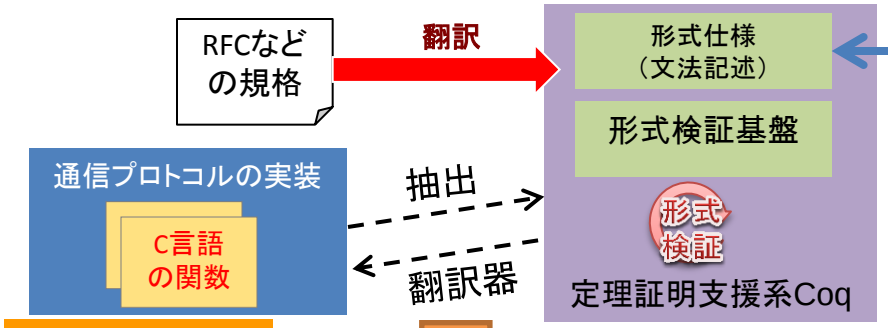
2．研究開発の目標

本研究開発では、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

通信プロトコルの安全の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

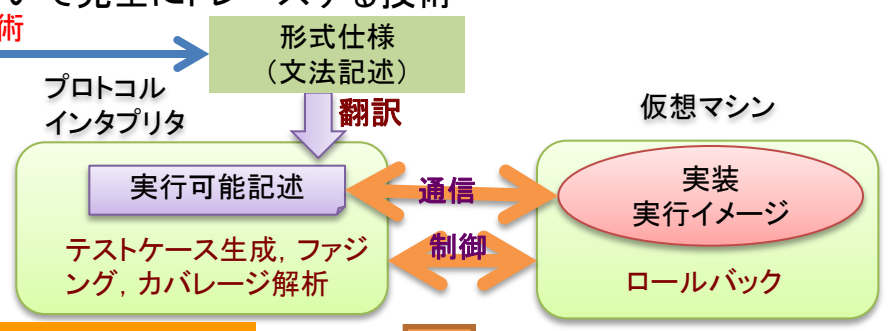


研究開発成果

(1) C言語の形式検証基盤を構築（定理証明支援系Coqで約15,000行）
⇒様々なC言語のプログラムの検証に応用可能
(2) TLSのインターネット標準の形式化
(3) 形式検証実験: PolarSSLのパージング関数(C言語約100行)を検証(約7,000行)
⇒PolarSSLの実装バグを発見

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

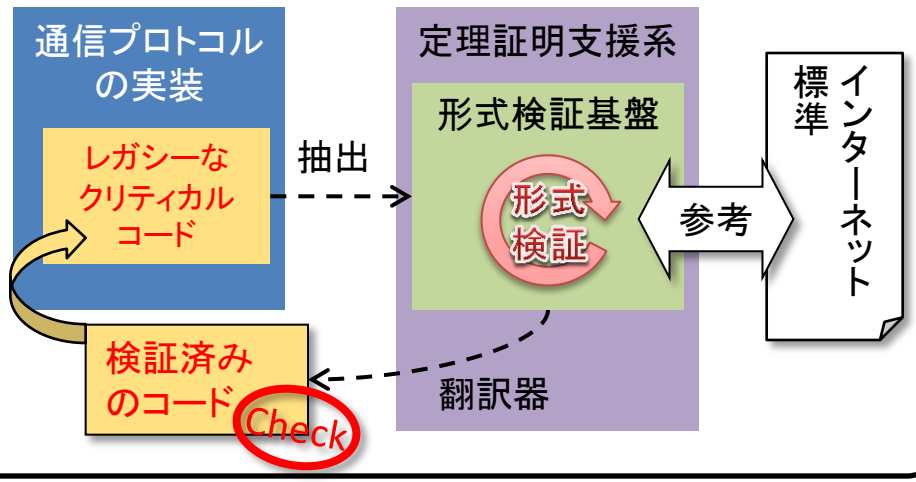


研究開発成果

(1) プロトコル記述言語策定、処理系を実装、TLSの仕様を形式的に記述
(2) 複数のOS/CPUで、TLSの実装(OpenSSL, GnuTLS, CyaSSL, PolarSSL)それぞれに約2,300回の網羅的ファジングテスト
⇒不具合発見(CyaSSL 2件, PolarSSL 1件)、開発者に報告、修正確認
(3) ロールバックによる反復ファジングテストの効率的実行を実現(約500msec/1ロールバック)

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



形式検証基盤の構築

定理証明支援系Coq

形式検証基盤

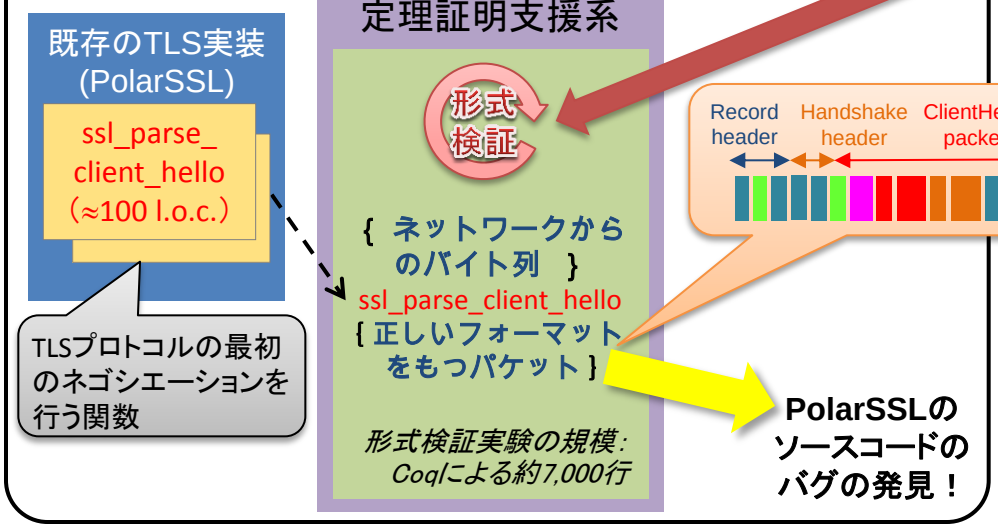
- 検証可能なプログラム → C言語
- 形式仕様 → ホーア＝トリプル:
  {事前条件}プログラム{事後条件}
- 形式体系 → 分離論理の拡張

形式検証基盤の規模:Coqによる約15,000行

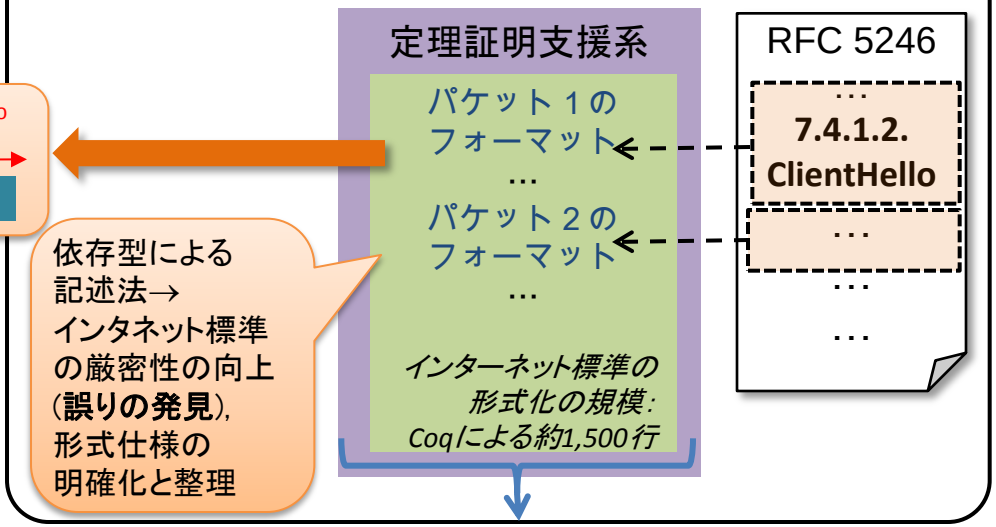
汎用性のある精密なモデル; 依存型による**コンパクト**な形式化

≈ 仕様と検証のための**定理群**

形式検証実験



インターネット標準の形式化

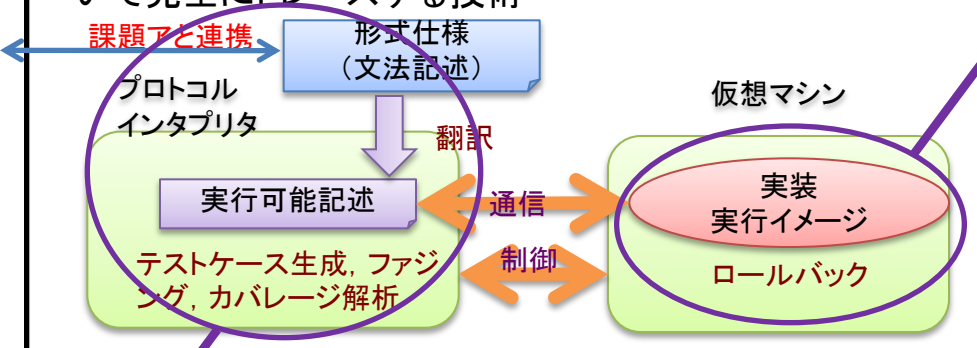


課題イと連携

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

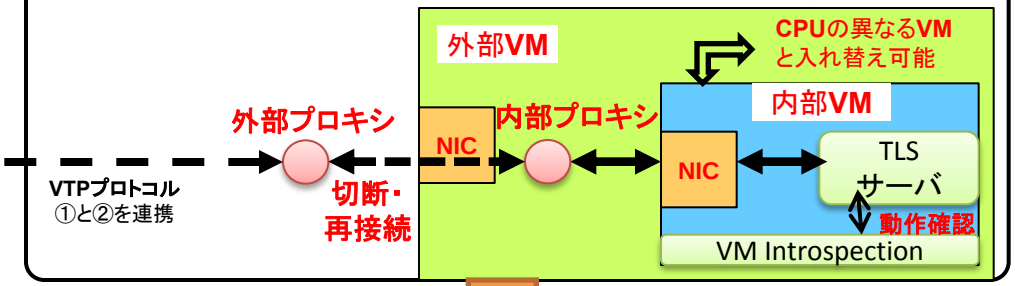
課題イ）網羅的テストケース生成による実装のブラックボックス解析技術の開発

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



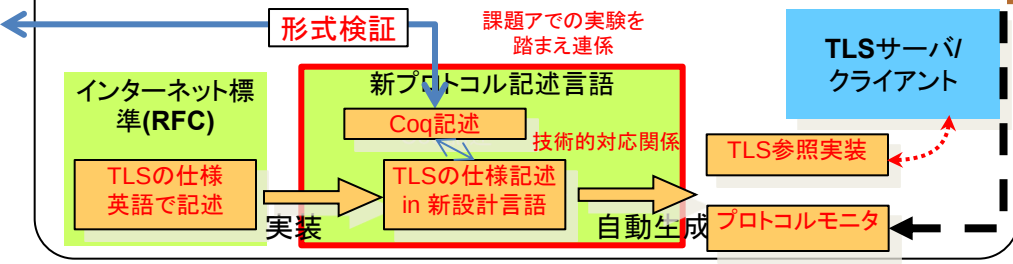
②二重VMによるロールバックとVM内部処理トレース技術

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。二重VMにすることで内部VMを他のCPUエミュレータと変更することも可能にし、X86およびARMのTLS環境をテストした。また、TLSの処理をトレースするVM Introspection機能(Virt-ICE)を内部VMに適用し、TLSがエラーハンドルルーチンに到達しているか確認できるようにした。



①プロトコル記述方式とリファレンス実装生成系

- これまでの仕様記述のわかりやすさを踏襲しつつ、
  詳細にプロトコル細部の記述のできる新仕様記述言語を策定
  - 仕様策定者向けの可読性と、実装者・検査者向けの正確性を両立
- 実際の TLS 1.2 の初期化部の仕様を新言語上で正確に記述
- 仕様記述を元に網羅的なファジング検査を実現、
  参照実装とプロトコル検査器を自動生成



複数のOS/CPU環境で4つのTLSサーバの実装を検査

- ①と②を連携・統合し、様々な環境で実装をテスト
  - 既存の4つのTLS実装
    (OpenSSL1.0.1c, GnuTLS3.1.5, CyaSSL2.4.2, PolarSSL1.2.3)
  - 2つのOS (Linux, Windows)
  - 2つのCPUアーキテクチャ (X86, ARM)
- ロールバックによる高速な反復ファジングテスト
  (X86-Linuxのロールバックで500msec/回)
- 1実装あたり約2,300ケースの網羅的テスト
- **3件の不具合を発見** (CyaSSL 2件,PolarSSL 1件)
  ⇒ 開発者に報告、修正を確認

4. これまで得られた成果（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	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	0	10(4)	0	4(4)	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
「ソフトウェアセキュリティ研究チームの活動報告」の発表内で本プロジェクトを紹介し、報告会に参加した企業および大学関係者と議論した。

第1回 セキュアシステムシンポジウム
日時：平成24年9月10日（月） 10:00～16:55　場所：みらいCANホール（日本未来科学館　7F）
招待講演：三菱電機株式会社　情報技術総合研究所情報セキュリティ技術部長　松井 充 氏
Google Inc. Google Chrome Team　Ian Fette 氏
講演「ソフトウェア信頼性向上のための形式技法・開発支援ツールの研究」およびポスター展示「形式仕様に基づくプロトコル実装の自動テスト」により、本プロジェクトで開発したブラックボックステストの自動生成ツールを説明し、シンポジウムに参加したセキュリティ企業と議論した。

産総研オープンラボ
日時：平成24年10月25.26日（木、金）13:30-18:00　場所：独立行政法人　産業行技術研究所　つくばセンター
ポスター展示「高信頼ソフトウェア開発プロセス支援ツールの研究」を通して、本プロジェクトで開発したプログラムが仕様通りに実装されていることを定理証明器Coqで厳密に証明する方法を多くの企業に紹介した。

6. 今後の研究開発計画

標準化に関して、TLS1.2の曖昧な仕様など実際に問題になる課題を選んでいるため、今後研究を進めることで仕様記述に関する標準化貢献が見込める可能性は高いと思われる。また、今回の開発ではIETFで公開しているRFCと親和性の良い設計を進めており、今後標準化コミュニティに対して有用性を示すことができると考える。知財に関しては、インターネットにおけるデファクト標準を想定対象としている面もあり、本研究の成果は知的財産として囲い込むのではなく、広く一般に公開し様々な通信プロトコルのデザインおよび実装の場面で利用される事が好ましいと考えてる。ただし、今回の知見としての成果は、公開した知財を活用したコンサルテーション業務で役立てていく予定である。また、仮想計算機環境の拡充などにより、ブラックボックス実装などのより面倒な検査対象への技術の適用を計る。