平成２４年度研究開発成果概要書
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（14801）
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」

（１）研究開発の目的

インターネット標準の現実の実装は、厳密な意味では仕様を満せていない場合が多い。暗号通信プロトコルなどにおいては、その仕様と実装のわずかなズレが脆弱性に繋がるケースが少なからず知られている。このような誤りは実装者の注意不足に起因する場合も多いが、原因の一端が標準の仕様記述そのものに内在する場合もある。

本プロジェクトでは、形式的手法による通信プロトコル仕様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追跡およ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。

（２）研究開発期間

平成２２年度から平成２４年度（３年間）

（３）委託先

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

（４）研究開発予算（百万円単位切上げ）

平成２２年度	４１（契約金額）
平成２３年度	３９（　〃　）
平成２４年度	３６（　〃　）

（５）研究開発課題と担当

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（産総研）

アーキテクチャに依存するC言語プログラムの検証を行うために、平成23年度は、基本的な型と表現のモデルに関する研究を行った。平成24年度はこの型と表現のモデルに基づき、Cの意味操作論、ホーア論理、および分離論理などに関する定理群を整備する。

また、平成24年度は、平成23年度に始めた既存実装のTLSパケットパージング関数のソースコードの検証実験を続ける。具体的には、上記の改良に基づき、平成23年度に行った予備実験の拡張を行う。アーキテクチャに依存する関数の形式モデルに基づく検証では、今までより長大な証明が必要になると予想

されるので、これを抑えるために証明の単純化に努める。

平成 23 年度に C 言語実装の形式検証基盤の限定的モデルを作成した。平成 24 年度はこの形式検証基盤の改良を続ける。具体的には、平成 23 年度に得た精密な型と表現のモデルを用いて、C の意味操作論、ホーア論理、および分離論理に基づく定理を拡張する。以上の改良を用いて、例えば、移植性を保つ関数の形式検証ができるようにする。

また、平成 24 年度は、平成 23 年度に始めた既存実装の TLS パケットパージング関数のソースコードの検証実験を続ける。具体的には、上記の基盤の改良に基づいて、平成 23 年度に行った予備実験を繰り返して、拡張する。精密な形式モデルに基づく検証実験により、多くの検証条件が出てしまうが、これを抑えるために定理の扱いを簡単にするように努める。

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

イ-1) 網羅的汎用テストジェネレータおよび実行環境

a. 網羅的プロトコル検査のためのプロトコル記述方式（産総研）

平成 23 年度には、課題(ア)における文法解析の理論解析の結果を基に文法定義言語を設計し、基本的な状態遷移言語と組み合わせて文法解釈・生成・プロトコル実行器を検査器の基本機能として設計し、レピダムと共同で実装した。平成 24 年度はこれを元に、言語の設計をより洗練し、仕様書としての可読性と利便性を高めると共に、自動的な疑似攻撃のために必要な情報について簡潔かつ十分な記述を目指して仕様の検討を行う。また課題(イ-2)で開発する実際のプロトコル処理のトレース・実行状態ロールバックとの連携のために、プロトコルの分岐可能性を網羅的にたどる手法についても効率性や追跡可能性等を考慮しながら開発・改良を行う。

b. 網羅的プロトコル検査のための処理系の開発（レピダム）

平成 24 年度は、産総研側で更に改良を進める(上記参照)プロトコル仕様記述言語について実装の詳細設計と実装作業を進める。また、ファジングなど疑似攻撃を行うための記述についても、実装の立場から言語デザインへの助言を行う。また、制作した処理系上で実行する TLS プロトコル仕様の記述を進め、課題(イ-2)における実行状態制御の仕組みと組み合わせ、既存の TLS などの実装の実行に対し疑似攻撃を含む通信を行い、不具合を発見するための技術を開発する。

イ-2) 仮想マシンベースとしたコントロールフロー解析（産総研）

平成 23 年度では、(イ-1)で規定された制御コマンドが埋め込まれたパケット

を受け取ると、その制御コマンドを分離する機能、制御コマンドによる仮想マシンの状態を操作(仮想マシンのスナップショットの取得やロールバック)する機能を作成した。現在の実装ではプロキシを利用しており、テストジェネレータで頻繁に制御コマンドを送った場合に性能の問題があるため、本年度は性能向上を行い、実用に耐えるようにする。

また、現在の実装は二重の仮想化(ネステッド VM)を使っている。そこでは内側の仮想マシンが交換可能なため、CPU エミュレートタイプの技術を適用すれば任意の CPU 上で動作するブラックボックスシステムの検査ができるように拡張する。

（６）これまで得られた研究開発成果

（累計）件　　（当該年度）件

特許出願	国内出願	0	0
	外国出願	0	0
外部発表	研究論文	0	0
	その他研究発表	10	4
	プレスリリース	0	0
	展示会	4	4
	標準化提案	0	0

具体的な成果

① ACM ワークショップ PLPV 2013 での発表（形式検証基盤の実現とその現実的な応用）

C 言語で実装されたプロトコル実装の正当性を形式検証する新たな基盤技術を開発し発表した。C 言語のサブセットで書かれた実装を扱うための形式定義と、TLS プロトコルの標準 RFC によるパケットフォーマットの形式化などを Coq 定理証明支援系上に検証基盤として構築し、その概要を発表した。また、全体の形式検証基盤の構成とその現実的な応用についても紹介した。この応用では、実際に RFC 標準の TLS パケット仕様と既存の TLS 実装の処理の一部 （PolarSSL の ClientHello パケットのパージング関数、約 100LOC） を正確に形式化し、その処理中で扱われるメモリ上のデータ構造を分離論理を用いて記述した上で、検証対象の関数が正しくデータを仕様に基づいて解釈し、メモリ領域に解釈結果を正確に記録していることを具体的に検証した。この検証のプロセスは約 7,000 行の証明ステップで行うことができた。

② 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（PPL2013）での発表（形式仕様記述言語の策定と網羅ファジングの実現）

昨年度着手した実装を元に、プロトコル形式仕様記述言語の詳細を決定した。実際にこの仕様記述言語を解釈し参照実装として動作させるインタプリタを作成し、さらにこの言語上で TLS 1.2 プロトコルの初期化部分を実際に記述し、既存の複数の実装と相互通信させることに成功した。このことにより、この形

式仕様記述言語が十分な記述性を持つことを確認した。続いて、このインタプリタの実装を工夫することにより、実行状態の分岐が管理できるようにしたうえで、プロトコル中の不正入力攻撃の可能箇所を網羅的に数え上げる機構を実装、また既存のファジング機構などを元に実際に不正入力を生成する仕組みと組み合わせることで、網羅的なファジング検査を実現する検査器の実装も行った。実際にこの機構で 2000 通り以上の不正な入力を生成し、③の成果と組み合わせることで効率的に検査をすることができるようになった。

③ ACM ASPLOS ワークショップ RESoLVE2013 での発表 (Nested VM とプロキシによる細粒度スナップショット・ロールバックの実現)

プロトコルのファジングテスト実行環境として、(1)パケットレベルのスナップショット・ロールバック、(2)乱数の再現性を含めたロールバックの必要性を明らかにし、その実行環境として二重の仮想化(Nested VM)とプロキシを使った実装を提案した。パケットを管理するプロキシと Nested VM を組み合わせることで、既存の VM が持つスナップショット機能を活用して汎用な実験環境が構築できることを示した。また、Nested VM では外部 VM を X86 の仮想命令を使う KVM、内部 VM に全命令をトレースする QEMU にすることで高速な実行ができることを示した。

（７）研究開発イメージ図

別紙参照

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）

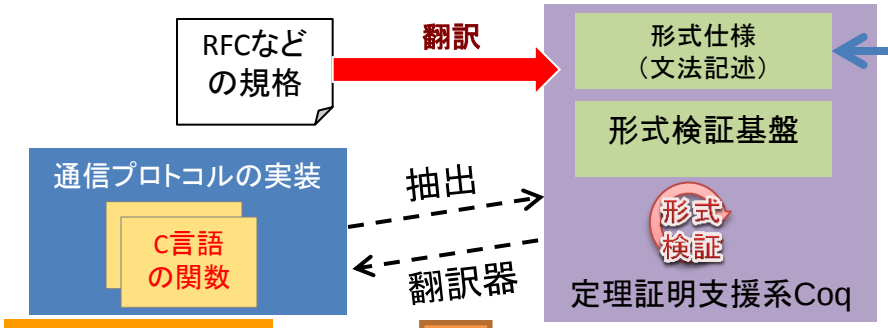
2．研究開発の目標

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

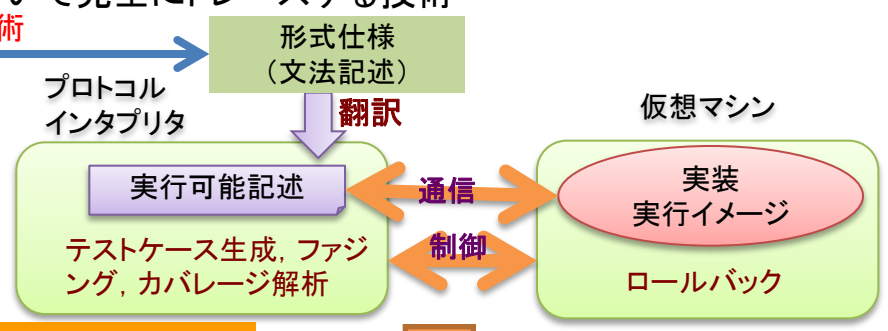


研究開発成果

(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

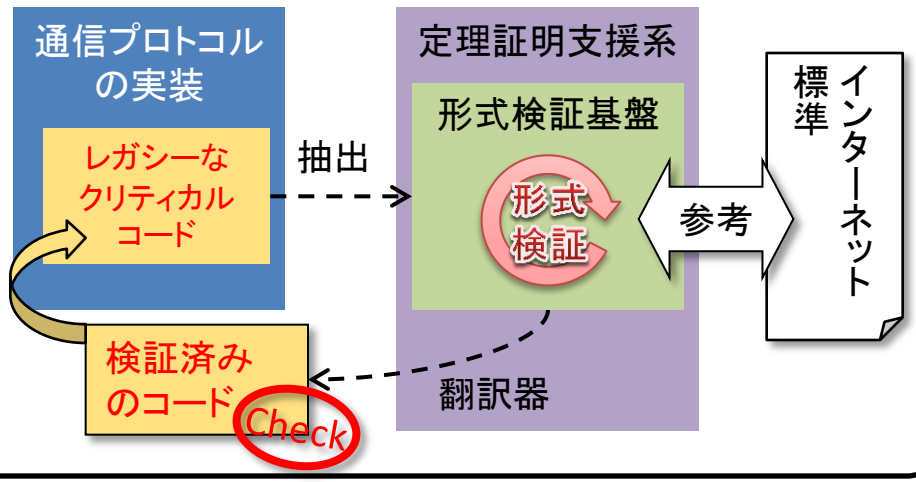


研究開発成果

(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

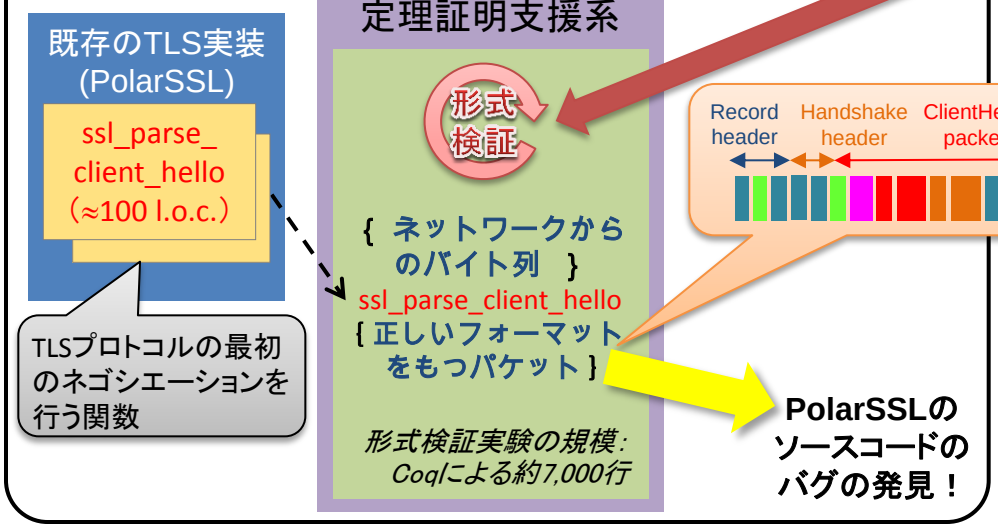
- 検証可能なプログラム → C言語
- 形式仕様 → ホーア＝トリプル:
  {事前条件}プログラム{事後条件}
- 形式体系 → 分離論理の拡張

形式検証基盤の規模:Coqによる約15,000行

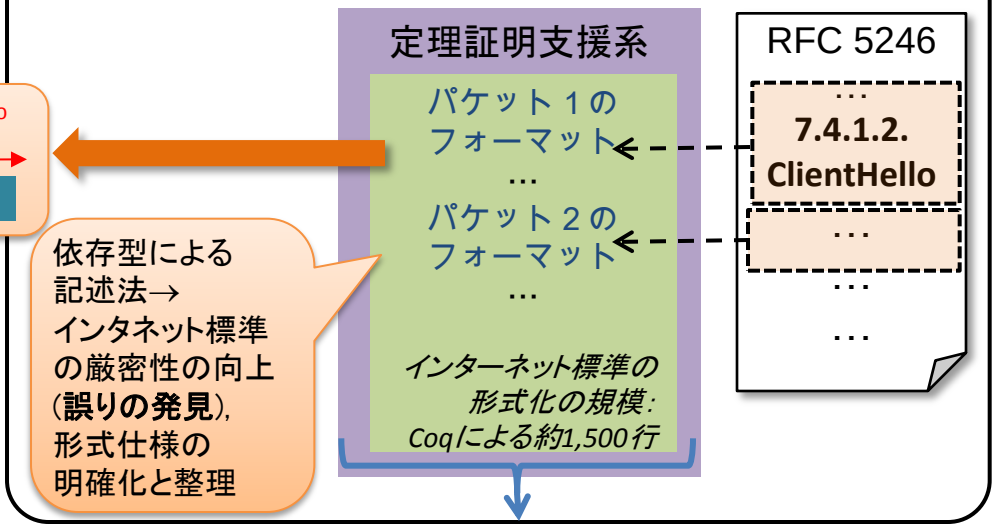
汎用性のある精密なモデル; 依存型による**コンパクト**な形式化

≈ 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

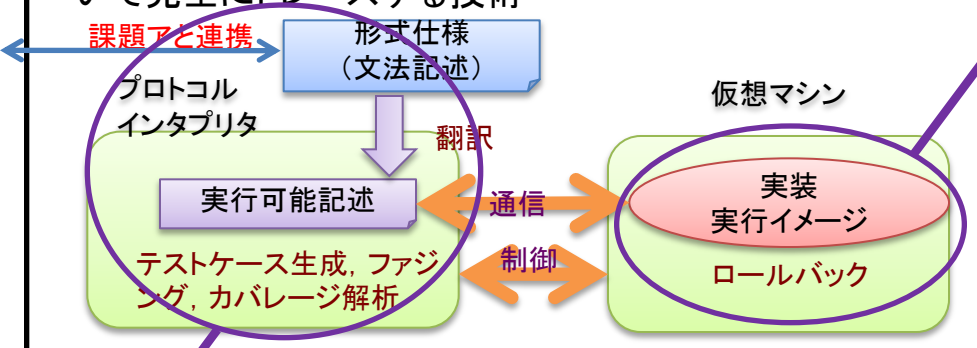


課題イと連携

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

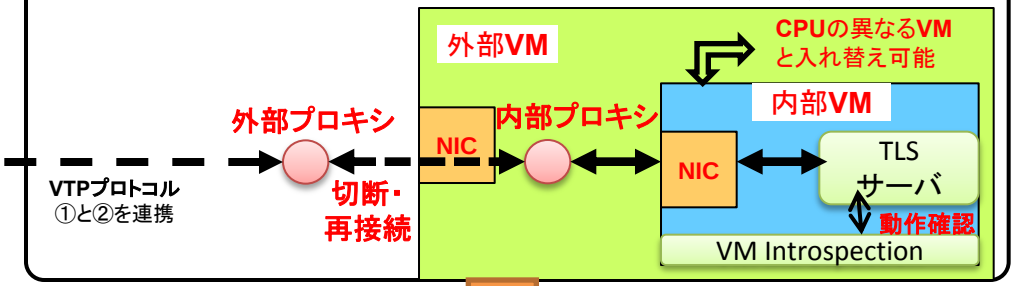
課題イ）網羅的テストケース生成による実装のブラックボックス解析技術の開発

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



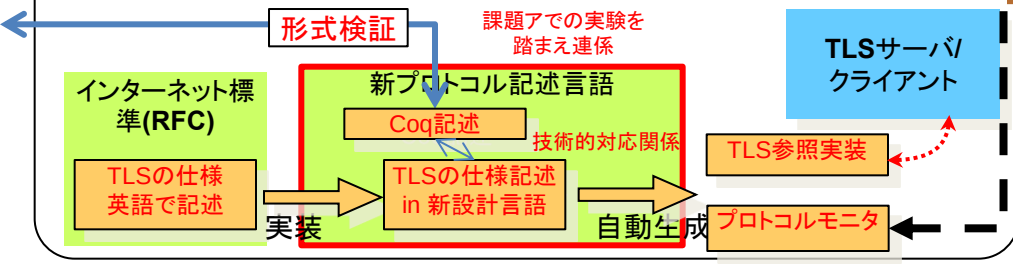
②二重VMによるロールバックとVM内部処理トレース技術

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。