平成２２年度 新規委託研究
「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」
研究計画書

独立行政法人 情報通信研究機構

１．研究開発課題

『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』

２．研究開発の目的及び内容

通信機器に実装された通信プロトコルが、意図せざる入力によって規格上想定されていない動作を行い、その結果、セキュリティインシデントや情報漏洩が発生しないようにするための解析手法の研究開発を行い、情報ネットワークインフラストラクチャを支える通信プロトコルの安全性を評価するシステムの構築を行う。内部構造の情報が網羅できないネットワークインフラストラクチャとその構成要素へのブラックボックス解析により、安全性を評価するシステムを構築する。

本研究は、装置の通信プロトコル（仕様等）そのものにミスがある場合の研究も実装にミスがある場合の研究も双方をその対象とする。想定される研究開発の例としては以下が考えられるが、この例に捉われることなく、上記目的に沿った研究開発の提案を歓迎する。

① ルータやモバイル機器に搭載されている通信プロトコルの実装の安全性を評価するための解析手法とこれを実装した安全性評価システムの構築。

② プロトコルに対する解析フレームワーク・評価システムの構築。対象とするプロトコルの例としては、普及し標準となっている基幹ルータ（情報インフラ）や組み込み機器で使われるプロトコル、アプリケーションレイヤで使われるプロトコル、またコネクション管理を行うプロトコル等が挙げられる。

③ 研究開発した解析手法と評価システムについての、標準化や解析プラットフォームの開発と展開等も視野に入れた普及活動。

３．研究開発期間及び予算

研究開発期間：契約締結日から平成２４年度までの３年間。

予算総額：平成２２年度は１５０百万円程度を上限とする。

（全採択提案の総額。採択予定件数は、３件程度である。なお、必要に応じて、各提案の予算額の調整を行った上で採択する提案を決定する場合がある。）

なお、平成２３年度以降は対前年度比で 6%削減した金額を上限として提案を行うこと。

４．研究開発の到達目標

提案者が具体的な到達目標を定め、その達成如何を評価する指標と併せて、提案書に記載すること。この到達目標は、本研究開発の成果である安全性評価技術・システムを

用いることによって、平成２５年度以降に、ルータ、モバイル機器等の通信機器の脆弱性を解消し、使用者や所有者が意図しない情報漏えいを未然に防ぎ、以て安心･安全なインターネット環境の構築に資するものとし、ひいては世界に先駆けて日本のインターネットの安全性の確保を目指すものであること。

５．研究開発の運営管理及び評価について

研究開発に当たっては、機構が招聘しているプログラムコーディネータ（注：任命までの間、情報通信セキュリティ研究センター）の指導・助言を受けていただくとともに、機構が自ら行っている研究との連携を適宜図っていただく。また、平成２４年度に事後評価を行う。

６．参考（研究課題の設定の背景及びその必要性）

情報通信ネットワークの安全性を確保するには、そのネットワークを構成する各要素（通信機器）のセキュリティが担保されていることが必要である。現状では、ネットワークを構成する各要素がセキュアであるという条件の下で、その組み合わせからなるシステムをセキュアに組む手法については広く検討されている一方、各構成要素自体がセキュアであるという条件自体に対する評価・検討は十分なもとのは言えない。

ルータ、モバイル機器等の通信機器の通信プロトコルは、IETF 等で規定され、それに準じて通信機器へ実装されているが、規格で規定されていない詳細な設定はベンダー独自の仕様で行われており、その全容は容易には確認できない。通信機器がセキュアであることを検証するためには、ソースコード、回路図といった内部構造などを完全に明らかにしたうえで、それを検証できることが求められる。しかし、現在広く一般に使用されている情報通信ネットワークの機能・機器は、内部の構造が完全に明らかになっていないものが多いと同時に、知的所有権保護などの法的な問題、あるいはライセンス料や検証コストなどの経済的な問題から、内部構造を明らかにすることは実質的には不可能であるといえる。

内部構造が明らかになっていない場合、安全性の確認のためには、複数の通信プロトコル、多種類の通信パケットの組み合わせから、極めて多くのテストパターンでの評価が必要となり、現実的な時間で実施することは困難である。また、規格自体に欠陥がある場合、その検証はきわめて困難である。現状では、１つの通信プロトコルに対するテスト評価ですら網羅的に行われておらず、通信機器導入の判断基準や動作確認手段がない。特に中小の ISP には、通信機器導入の判断基準や動作確認手段がない。

このため、不適切な通信プロトコル実装に伴う情報漏えい等が発生していないかを確認する技術及びシステムと解析評価手法を開発し、広く一般にその成果を利用することが、ICT システム全体の情報セキュリティの確保のために必要である。そのための情報システムの安全性評価や、情報漏洩を引き起こす入力を含むパターンの生成を行うための境界値分析、またその自動化のための手法（ファジング等）の研究開発を行

う。

上記２．で示した研究内容を具体例としては、以下が想定されるが、この例に捉われることなく、上記目的に沿った研究開発の提案を歓迎する。

(1) 通信プロトコルそのものに安全上の課題がある場合を研究対象とするとき

①通信プロトコルの安全性の評価手法。

② 規格標準化され、普及しているプロトコルの安全性評価手法。

③ 比較分析、境界値分析アルゴリズムの研究開発（入出力パケットの挙動を体系的・網羅的に比較分析する数学的アルゴリズム）。

(2) 通信プロトコル自体ではなく、その実装に安全上の課題がある場合を研究対象とするとき

④基幹ルータや組み込み機器で使われる、IPV6、TCPIP、BGP の実装運用方法の脆弱性解析手法と評価フレームワーク

⑤アプリケーションレイヤで使われる IP Telephony、Web 関連システムの実装・運用方法の脆弱性の解析手法と評価フレームワーク

⑥コネクション管理を行う MPLS、GMPLS 等の実装・運用方法の脆弱性解析手法と評価フレームワーク

⑦P2P のプロトコル、インターフェイスの実装に関する脆弱性解析手法と評価方法

⑧特定、独自のプロトコルの実装に対応可能な脆弱性解析手法と評価方法

⑨ルータ、組み込み機器の情報表示、ブラウザに関するプロトコルの実装に関する脆弱性解析手法と評価フレームワーク

⑩上記⑨を自動化するための手法（ファジング関連）

⑪近年セキュリティの脆弱性が多々指摘されている無線通信プロトコルの実装運用方法の脆弱性解析手法と評価フレームワーク

⑫近年普及が進んでいる TPM（Trusted Platform Module）のプロトコル、インターフェイスの実装に関する脆弱性解析手法と評価方法

また、本委託研究で扱う内容は、情報通信研究機構情報通信セキュリティセンターの研究内容と相補的な関係になっており、本委託研究での成果物を用いて、情報通信セキュリティセンターで研究開発を行っている安全な実装方式や別形式の脆弱性解析手法を評価することがある。