様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 １５ 日現在

機関番号：１３９０１
研究種目：若手研究(B)
研究期間：2016～2019
課題番号：１６Ｋ２１０９７

研究課題名（和文）IoTを支える高信頼組込みシステム向けセキュリティ脅威分析支援システム

研究課題名（英文）Security threat analysis system for highly reliable embedded / IoT systems

研究代表者
松原　豊（Yutaka, Matsubara）

名古屋大学・情報学研究科・准教授

研究者番号：３０５４７５００

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：本研究では，高信頼組込みシステムの安全性とセキュリティを両立するために，脅威分析手法の確立と，それを支援するコンピュータシステムの構築，セキュリティ対策手法の試作を目的とした。セキュリティ脅威の分析を支援するシステムとして，過去に見つかっている脅威リストから導出される キーワードをデータベース化し，分析対象のシステムの設計情報に対して，半自動的にキーワードを適用することで，人手による脅威分析を支援する手法を開発した。システムの設計段階で対策を組み込むために，既存の対策技術もデータベース化し，ファジング手法については試作も踏まえて，設計を支援する仕組みを構築した。

研究成果の学術的意義や社会的意義
本研究の対象とした，自動車，鉄道や宇宙機など高信頼性を要求されるIoT/組込みシステムは，本国における主要産業の一部であり，その安全性とセキュリティを両立するための基礎技術は，それらの産業分野の根本を支える意味で，社会的な意義は非常に高いものと考える。加えて，特にセキュリティの脅威分析や対策技術の検討は，人的なリソースが不足する状況において効率化するためには，自動化することが欠かせない。本研究では，学術的にも競争の激しい，この分野に挑戦し，一定の成果を上げることができた。

研究成果の概要（英文）：The purpose of this study is to establish a threat analysis method, to construct a computer system to support it, and to prototype a security countermeasure method in order to achieve both safety and security of the highly reliable embedded system. As a system that supports the analysis of security threats, a keyword derived from a list of threats found in the past is compiled into a database, and the keywords can be semi-automatically applied to the design of the system to be analyzed. In order to incorporate countermeasures at the system design stage, existing countermeasure technology including fuzzing testing was included into the database.

研究分野：組込みシステムの安全性とセキュリティ

キーワード：組込みシステム　安全性　セキュリティ

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

ソフトウェアが搭載された高度な組込みシステム（例えば，自動車制御システム，FA 機器，ロボット制御システム，航空機制御システム等）の安全性確立手法は，従来から個々の企業に蓄積された知見・経験に加えて，業界・分野ごとに国際規格が整備されつつあり，基礎技術の普及が進んでいる．例えば，機能安全国際規格は，2005 年に発行された IEC 61058 第１版により基本的な考え方が浸透し，2011 年に自動車制御システム向け規格 ISO 26262，2014 年に生活支援ロボット ISO 13482 がそれぞれ正式に発行された．

組込みシステムの高機能化，クラウドとの連携が進むにつれ，電話回線やインターネットなどの外部ネットワークを介して提供するサービスが増えつつある．その一方で，セキュリティを侵害する脅威も高まっている．その結果，安全性は考慮しているがセキュリティ上の脅威への対策が不十分な組込みシステムの脆弱性を指摘する研究発表が急速に増加している．

組込みシステムのセキュリティを確立するためには，外部からの意図的な操作，攻撃などの脅威への対策を，システムの設計段階で組込み，運用時にも継続して脅威分析を実施することが必要とされるが，現時点ではその具体的な手法が確立していないことが大きな課題となっている．これを解決するためには，組込みシステムの専門知識に加えて，安全性確立手法の知識も必須であることから，研究者・技術者が不足している．その結果，特に組込みシステムのセキュリティの脅威を網羅的に分析する手法の研究が急務となっている．

２．研究の目的

組込みシステムの安全性とセキュリティを両立するために脅威分析手法の確立と，それをコンピュータにより支援するシステムの構築を目的とした．研究代表者らがこれまで研究してきた，安全分析手法，安全システム構築技術を基に，組込みシステム（特に，自動車制御システムとロボット制御システム）を対象として，脅威分析手法，セキュリティの脆弱性評価方法，人手による脅威分析の支援・自動化システムの構築の 3 つのサブテーマを実施することが特徴である．組込みシステムのソフトウェアプラットフォーム，安全性の確立手法の両分野に精通した研究者・技術者は少なく，それらをベースにセキュリティの確立を目指すというアプローチで研究を実施できる研究者は，日本国内においてはほとんどいないため，本研究の意義，独創性は高いと考えている．セキュリティの確立においては，多様な視点をもつ研究者，技術者が協力することが重要である面もあるため，研究成果に関しては，情報セキュリティの専門家とも積極的に議論して，世の中に還元したいと考えている．セキュリティの確立手法は，特定のシステムに限定されるものではないことから，IoT（Internet of Things），組込みシステムとクラウドの連携等，近い将来に登場する技術にも応用可能であると考える．この意味で，本研究の学術的な意義も非常に大きいと考える．

３．研究の方法

①組込みシステム向けの脅威分析手法の開発

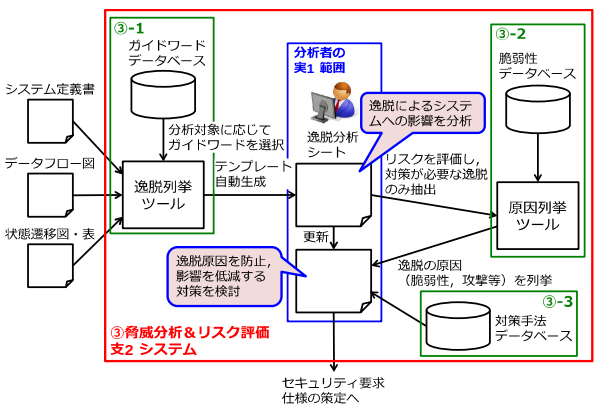
研究代表者らが開発した HAZOP ベースの安全分析手法を拡張させて，組込みシステムを対象として，脅威分析手法を提案する．その分析能力を評価するため，我々の手法を使って，過去のセキュリティインシデントで報告されている攻撃手法を実際に発見できることを確認した．

②組込みシステムにおけるセキュリティの脆弱性評価手法の開発

組込みシステム（特に，自動車制御システムとロボット制御システム）を対象として，システムの脆弱性を定量的に評価する基準の素案を構築し，リスク評価を試みた．CVSS を基に，評価項目を組込みシステムに特化した脆弱性評価手法を開発した．

③脅威分析支援システムのプロトタイプ開発

①と②で開発した手法をツール化し，コンピュータによって脅威分析を支援するシステムのプロトタイプを構築した．脅威分析を支援するシステムがあれば，負荷を大幅に減らすことができると考えられる．小規模な組込みシステムに適用し，人手により実施する分析の結果と同等以上の結果が得られることを確認する．



本研究のゴール：脅威分析＆リスク評価支援システム

４．研究成果

本研究では, これまで研究代表者が研究してきた, 安全分析手法, 安全システム構築技術を基に, 組込みシステム（特に，自動車制御システムとロボット制御システム）を対象として，脅威分析手法，セキュリティの脆弱性評価方法，人手による脅威分析の支援・自動化システムの構築の 3 つのサブテーマを実施した．研究成果の一部だけであるが，学術論文，研究会，展示会，ウェブサイト等で，無償で公開した．今後は，脅威分析支援システムの改善と，セキュリティ対策技術の研究・開発を継続し，オープンソースとして公開することを目指す。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計9件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 長柄啓悟，松原豊，高田広章
２．発表標題 ブロックチェーン技術を用いたIoT機器向けセキュアアップデートフレームワーク
３．学会等名 組込みシステムシンポジウム2018
４．発表年 2018年

１．発表者名 河田智明，本田晋也，松原豊，高田 広章
２．発表標題 Arm TrustZone for Armv8-M を利用したマルチタスク対応 CFI の検討
３．学会等名 組込みシステムシンポジウム2018
４．発表年 2018年

１．発表者名 小松大河，松原豊，高田広章
２．発表標題 IoT機器への適用に向けたTLS1.3の性能評価
３．学会等名 コンピュータセキュリティシンポジウム2018
４．発表年 2018年

１．発表者名 河田 智明，本田 晋也，松原 豊，高田 広章
２．発表標題 Shadow exception stacks: 非同期例外を対象とした TrustZone-M ベースの CFI 機構
３．学会等名 暗号と情報セキュリティシンポジウム
４．発表年 2019年

１．発表者名
長柄啓悟，青木克憲，松原豊，高田広章

２．発表標題
組込みシステム向けのポータブルDoSテストツール

３．学会等名
組込みシステムシンポジウム（ESS2017）

４．発表年
2017年

１．発表者名
青木克憲，松原豊，高田広章

２．発表標題
組込みネットワークスタックlwIPを題材としたバグ検出を支援するシンボリック実行環境

３．学会等名
2018年暗号と情報セキュリティシンポジウム

４．発表年
2018年

１．発表者名
Keigo Nagara, Katsunori Aoki, Yutaka Matsubara , Hiroaki Takada

２．発表標題
Open-source software-based portable DoS test tool for IoT devices

３．学会等名
Workshop on Internet of Things Security and Privacy Collocated with ACM CCS（国際学会）

４．発表年
2017年

１．発表者名
Jingxuan Wei, Yutaka Matsubara, Hiroaki Takada

２．発表標題
An Aiding Tool for HAZOP-based Analysis for Embedded Systems

３．学会等名
第14回クリティカルソフトウェアワークショップ（WOCS2）

４．発表年
2016年

１．発表者名 長柄啓悟，松原豊，青木克憲，高田広章
２．発表標題 組込みシステム向けマルウェア Mirai の攻撃性能評価
３．学会等名 情報処理学会研究報告
４．発表年 2017年

〔図書〕　計1件

１．著者名 Jingxuan Wei, Yutaka Matsubara, Hiroaki Takada	４．発行年 2016年
２．出版社 HAZOP-Based Security Analysis for Embedded Systems: Case Study of Open Source Immobilizer Protocol Stack", Springer Recent Advances in Systems Safety and Security	５．総ページ数 262
３．書名 Recent Advances in Systems Safety and Security	

〔産業財産権〕

〔その他〕

研究代表者のウェブサイト https://sites.google.com/site/yutakaertl/publications

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考