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　５ 年　 ６ 月 ２７ 日現在

機関番号：８２７２３
研究種目：挑戦的研究（萌芽）
研究期間：2019～2022
課題番号：１９Ｋ２１５７３

研究課題名（和文）ロボット用オープンソースソフトウエアの悪用を防止する国際的枠組みの提案

研究課題名（英文）Proposal for an International Framework to Prevent the Abuse of Open Source Software for Robots

研究代表者

辻田　哲平（Tsujita, Teppei）

防衛大学校（総合教育学群、人文社会科学群、応用科学群、電気情報学群及びシステム工学群）・システム工学群・准教授

研究者番号：４０５５４４７３

交付決定額（研究期間全体）：（直接経費）　　4,900,000円

研究成果の概要（和文）：ロボット用オープンソースソフトウェア（OSS）のテロ等への悪用を防止する新たなフレームワークを提案した．一般に，OSS開発者はソースコードを公開サイトにて公開し，利用者はこれをそのまま又は一部改変して使用している．ソースコードを公開しているため，プログラム中に悪用防止機能を持たせても，その部分を除外するだけで簡単に悪用されてしまう．そこでCPU(中央演算処理装置）内部にOSSの実行コード検知機能を有するロボット用プロセサを試作し，これを搭載した車輪型移動ロボットで，実行可能エリアでのみプログラムを実行可能とする枠組みの実証実験を行った．

研究成果の学術的意義や社会的意義
ソフトウエアのソースコードを無償で配布・改良・再配布するといったOSSの考え方に賛同した開発者が多くのソフトウエアを公開し，お互いに改良することで，ロボット技術や人工知能技術に目覚ましい発展をもたらしている．これらの技術の社会的有用性は非常に高いが，悪用された場合，多くの被害をもたらすことが恐れられている．本研究は，OSSによって生み出されてきたロボット技術や人工知能技術が高度化し，人間社会の破壊に利用されかねない状況にある新局面において，高度な科学技術をコントロールするための枠組みを提案するといった社会的意義を有する．

研究成果の概要（英文）：We proposed a new framework to prevent the abuse of open source software (OSS) for robots for terrorism and other purposes. Generally, OSS developers release their source code to the public, and users use the code as is or with some modifications. Because the source code is open to the public, even if an anti-abuse function is included in a program, it can be easily abused by simply excluding that part of the program. To solve this problem, we developed a prototype robot processor with an OSS executable code detection function inside the CPU (central processing unit), and conducted a demonstration experiment using a wheeled mobile robot equipped with this processor to test a framework that enables program execution only in the executable area.

研究分野：ロボット工学

キーワード：オープンソースソフトウエア　悪用防止　ロボット　テロ対策

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

近年発達が目覚ましいオープンソースソフトウエア（OSS）はインターネット上で公開されており，誰でも利用できる．高度なロボット技術や人工知能技術も公開されており，悪意を持った者が容易に利用できる．このようにOSSが人間社会の破壊に利用されかねない新局面において，OSSの悪用を防止する枠組みを考える必要がある．OSS開発制度の社会的利点を損なわず悪用を防止することは，制度か技術のいずれかの取り組みだけでは為し得ない難易度の高い挑戦的な課題である．そこで，ロボット工学，国際法，ソフトウエア工学の専門家が密に連携し，国際団体の設立と悪用防止プロセッサの開発など，制度と技術を組み合わせた解決策を検討する必要がある．

２．研究の目的

ソフトウエアのソースコードを無償で配布・改良・再配布するといったOSSの考え方に賛同した開発者が多くのソフトウエアを公開し，お互いに改良することで，ロボット技術や人工知能技術に目覚ましい発展をもたらしている．これらの技術の社会的有用性は非常に高いが，悪用された場合，多くの被害をもたらすことが恐れられている．そこで，OSS 開発制度がもたらす社会的有用性を阻害せず，テロ行為等に利用される可能性を低減する枠組みを提案する．ロボット・情報工学の自由な発展を妨げず，悪用を制限する方法を研究者自らが解決を目指す．このように，OSS 開発環境によって生み出されてきたロボット技術や人工知能技術が高度化し，人間社会の破壊に利用されかねない状況にある新局面において，高度な科学技術をコントロールするための枠組みを提案することが目的である

３．研究の方法

本研究では，まず想定される規制方法について検討を行い，この枠組みのなかでコアとなる，悪用防止機能を有するロボット用プロセッサを試作し，実証実験を行った．

３．１　悪用防止フレームワークの検討

現在，OSS開発者はソースコード公開サイト(GitHub 等）に公開し，利用者はこれをそのまま又は一部改変して使用している．ソースコードを公開しているため，プログラム中に悪用防止機能を持たせても，その部分を除外するだけで簡単に悪用されてしまう．そこで広く流通しているCPU(中央演算処理装置）内部に外部からの改ざんを防止した領域に悪用防止機能を持たせ，対象プログラムを許可エリアでのみ実行可能とする．これにより重要施設や人口密集地域でテロを防止する枠組みを提案する．

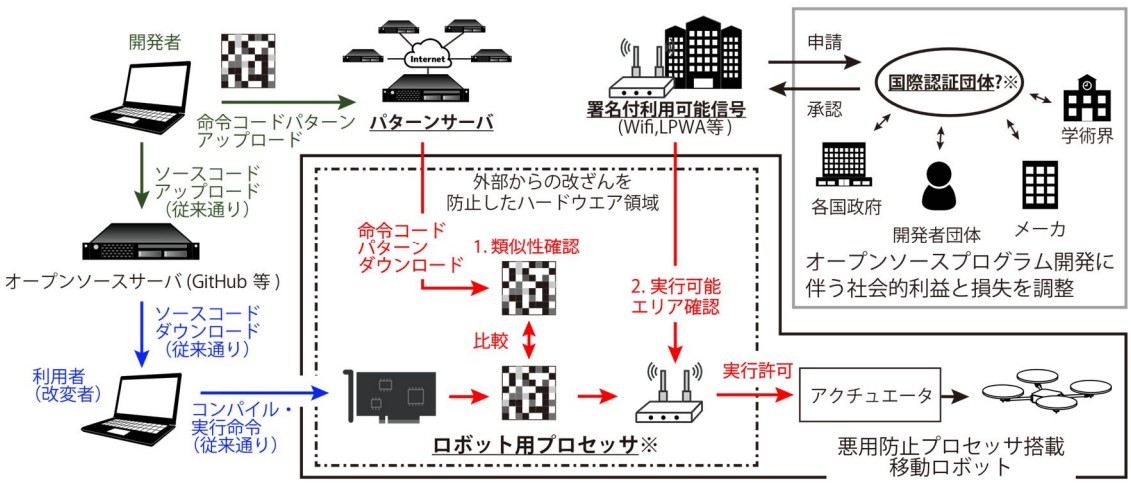

図１ ロボット用オープンソースソフトウエアの悪用防止フレームワーク

図１に示すように，開発者は自身の判断に基づき，プログラムの命令コードのパターンをパターンサーバに登録する．また開発者は後述する認証団体が設定する実行可能エリアの選択肢のなかから，自身のプログラムの実行可能エリアを良心に沿って選択する．ロボット用プロセッサ

は，実行するプログラムの命令コードパターンを，インターネットを介してパターンサーバから取り寄せたパターン一覧と照合する．類似度が高い場合，実行場所の確認を行い，実行可否を判断する．ここで，実行可能エリアの選択肢は，ロボット検証特区，学術研究機関，実行許可を希望する商業施設等を想定している．施設管理者は，新たに設置する学術界，メーカ，開発者団体，各国政府などからなる国際認証団体に申請し承認を受けて実行可能無線信号を対象エリアに送出することで，ロボット用プロセッサに実行可能エリアの判断を可能とさせる．

３．２　悪用防止機能を有するロボット用プロセッサの試作

前節で示した本研究で考案した提案フレームワークにおいてコアとなる，悪用防止機能を有すロボット用プロセッサの実現可能性を検証した．

(a) OSS の命令コードパターンの照合
前述の通り，プログラム中に悪用防止機能を持たせても，その部分を除外するだけで簡単に悪用されてしまう．そこで，プロセッサに流れる命令コードを別なプロセッサで読み取り，その類似度を判断することで，照合を行う枠組みを試作した．

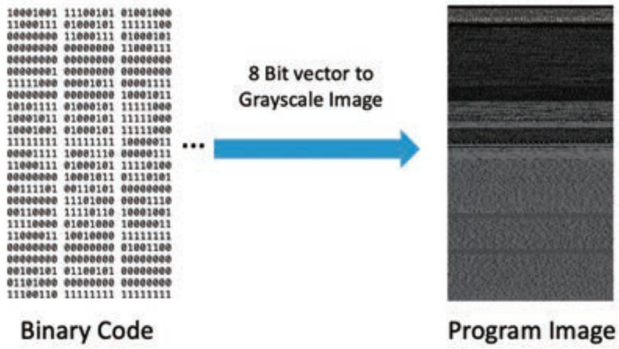

図 2 命令コードの画像化

図 2 に示すように，命令コードを画像化しその特徴量による判別を試みた．Intel 社製 FPGA (Field Programmable Gate Array)上で動作するソフトウエアプロセッサ Nios II 用のソフトウエアを複数種類用意し，k 近傍法で分類を行ったところ正しく分類されることが確認できた．

(b) 実行停止機能の実装
実行禁止エリアにおいて，プロセッサを強制的にリセットすることでロボットの動作を妨げる機能の実装を行った．

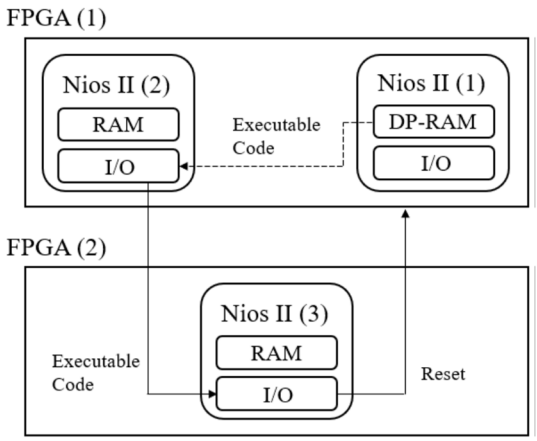

図 3 実行停止機能の構成図

図 3 に示すように，二つの FPGA を用いて実装を行った．Nios II(1)がユーザーがロボット制御プログラムを実行させるプログラムであって，Nios II(2)によって Nios II(1)で実行される実行コードを抜き出し，Nios II(3)に転送する．Nios II(3)で特定のコードを検知した場合は，FPGA(1)をリセットさせることで，Nios II(1)の実行を停止する．

４．研究成果

悪用防止フレームワークの実証実験を行うために，図 4 に示す悪用防止機能を有するロボッ

ト用プロセッサを搭載した車輪型移動ロボットを開発した.

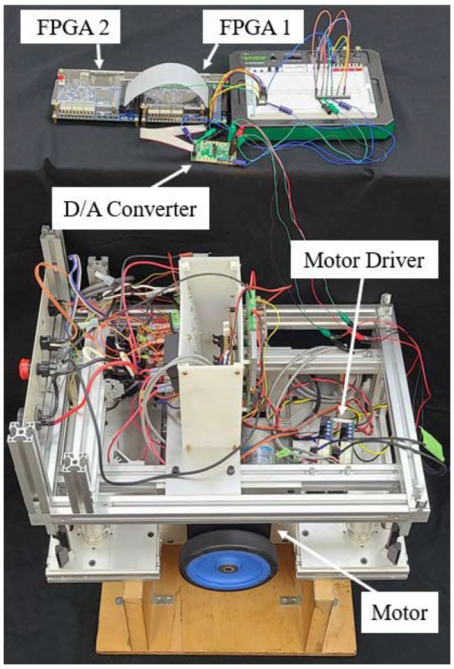

図 4 悪用防止機能を有するロボット用プロセッサを搭載した車輪型移動ロボット

本ロボットを用いて，屋外環境下で実験を行った．プログラム実行禁止エリアには東京都市大学世田谷キャンパスの A 地区（北緯 35.881 度以北）を設定した．ユーザーが実行可能エリアである東京都市大学世田谷キャンパスの B 地区から A 地区に向かって，左右独立駆動型移動ロボットの走行を開始させた場面を想定する．実行禁止エリアの判定には，GPS を用い，このとき，実行禁止エリアである A 地区に侵入したときにセキュアプロセッサがロボットを強制的に停止させられることを確認した．図 5 に検証実験の様子を示す.

(a) 通常動作時　　(b) 実行禁止エリアでの強制停止

図 5 実証実験の様子

また，近年その悪用の危険性が広く議論されている UAV (Unmanned Aerial Vehicle)についても，飛行体に求められる停止方法についても検討を行いながら，UAV 用のコントローラも試作した.

これらの成果について，東京大学未来ビジョン研究センターAI ガバナンスプロジェトと PwC コンサルティング合同会社が主催する AI と DEI 研究会 第 8 回「AI 活用とセキュリティ」において，研究代表者の辻田と研究分担者の佐藤が講師として紹介し，産業界，学術界，行政分野の参加者と高度な科学技術をコントロールするための枠組みについて議論を行った.

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 橋本洸，佐藤大祐，辻田哲平，安孫子聡子
２．発表標題 オープンソースソフトウェアを用いたロボットの悪用を防止可能なセキュアプロセッサの試作
３．学会等名 日本機械学会ロボティクス・メカトロニクス講演会
４．発表年 2022年

１．発表者名 辻田哲平，飯田裕貴，山田俊輔
２．発表標題 移動ロボットに搭載可能な非接触金属物体形状可視化装置の比較
３．学会等名 日本ロボット学会学術講演会
４．発表年 2021年

１．発表者名 辻田哲平，佐久間 大，山田俊輔，江藤亮輔，黒崎将広
２．発表標題 国際人道法に沿った歩哨ロボット用運用規制フレームワークの検討
３．学会等名 日本ロボット学会学術講演会
４．発表年 2021年

１．発表者名 田中涼，安孫子聡子，辻田哲平
２．発表標題 クアッドチルトロータUAVの開発効率化のためのRADフレームワークの構築
３．学会等名 日本機械学会ロボティクス・メカトロニクス講演会
４．発表年 2022年

１．発表者名
橋本 洸，石神 雄太郎，佐藤 大祐，辻田 哲平，安孫子 聡子

２．発表標題
オープンソースソフトウェアの悪用を防止可能なロボット開発フレームワークの提案

３．学会等名
第21回計測自動制御学会システムインテグレーション部門講演会

４．発表年
2020年

１．発表者名
冨沢 哲雄，佐久間 大，江藤 亮輔，山田 俊輔，黒崎 将広，辻田 哲平

２．発表標題
動的な混雑環境における自動検問ロボットの最適移動戦略

３．学会等名
第38回日本ロボット学会学術講演会

４．発表年
2020年

１．発表者名
坂井祐将，安孫子聡子

２．発表標題
クアッドチルトロータUAVのシームレス90 度姿勢遷移飛行の実飛行検証

３．学会等名
日本機械学会ロボティクス・メカトロニクス講演会2020

４．発表年
2020年

１．発表者名
Satoko Abiko and Tomohiro Harada

２．発表標題
Autonomous Flight of a Quad Tilt-rotor UAV at Constant Altitude

３．学会等名
23rd CISM IFToMM Symposium on Robot Design, Dynamics and Control（国際学会）

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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
研究分担者	佐藤　大祐 (Sato Daisuke) (40344692)	東京都市大学・理工学部・准教授 (32678)	
研究分担者	安孫子　聡子 (Abiko Satoko) (40560660)	芝浦工業大学・工学部・教授 (32619)	
研究分担者	黒崎　将広 (Kurosaki Masahiro) (10545859)	防衛大学校（総合教育学群、人文社会科学群、応用科学群、電気情報学群及びシステム工学群）・人文社会科学群・教授 (82723)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関