先端科学技術研究科　修士論文要旨

所属研究室 （主指導教員）	サイバーレジリエンス構成学 （門林　雄基　（教授））		
学籍番号	2411227	提出日	令和 8年 1月 18日
学生氏名	野口　真生		
論文題目	RISC-Vを使用したIoT機器に対するROP攻撃緩和策についての提案		

要旨

ROP（Return-Oriented Programming）攻撃は，スタック上の戻りアドレスを改ざんし，プログラム中に存在する既存の実行可能な命令断片（ガジェット）を連鎖的に実行させることで意図する任意のコード実行を可能にする手法である．近年，IoT機器への普及が期待されている命令セットアーキテクチャのRISC-Vは，セキュリティ防御機構の開発・実装が発展途上にある．特に，ROP攻撃に対して高い防御効果を持つとされるCFI（Control Flow Integrity）は，RISC-Vにおいて標準的に適用されていない．さらに，CFIはプログラム全体の制御フローを実行時に常時監視・照合する必要があるため，計算資源に制約のあるIoT機器のような低リソース環境への適用は困難であるとされている．

本研究ではRISC-Vを対象とし，IoT機器のようなリソースに制約のある環境下においても適用可能な，軽量かつ実用的なROP攻撃緩和手法を提案する．提案手法では，コンパイル後のサニタイズされたアセンブリコードに対して命令の挿入および使用レジスタの静的な変更を行う．本手法の特徴は，攻撃者がROP攻撃コードを構築する際に不可欠となる「ガジェット検出ツール」の検出アルゴリズムの正常な動作を阻害する点にある．具体的には，プログラムの論理的な動作に影響を与えない程度の冗長な命令列を意図的に挿入することで，検出ツールがバイナリを走査するプロセスを乱し，ガジェットの正確な検出を困難にする．これにより，ROP 攻撃におけるガジェット特定を困難にし，攻撃難易度を上昇させることを目的とする．