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　６ 年　 ５ 月 ３１ 日現在

機関番号：２７３０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2023
課題番号：１９Ｋ１１９６８

研究課題名（和文）サイバー攻撃による異常動作検知機能を持ったプロセッサの開発

研究課題名（英文）Development of a processor with anomaly detection functions against cyber attacks

研究代表者
加藤　雅彦（KATO, MASAHIKO）

長崎県立大学・情報システム学部・教授

研究者番号：００５３６４９３

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：1)CPUの異常動作検知に有効なCPU内部情報は、実行アドレス、L1命令キャッシュ及びL1データキャッシュのヒット率(全体、カーネル空間、ユーザ空間)である。2)小型のハードウェアに機械学習回路を実装するには、ランダムフォレストが適している。3)CPU実装に影響を及ぼさない小規模回路で、本機能を実装可能である。4)特徴を損なわないビット幅削減や割り算表などによる計算量削減により、判定結果に影響しないよう回路規模の縮小、消費電力の削減ができる。5)ハードウェア実装された機械学習回路を再学習させることができる。6)小規模なFPGAを搭載したハードウェアで実際に動作させることができた。

研究成果の学術的意義や社会的意義
本研究は小規模なプロセッサで動作しているIoT機器に対して、アンチウイルスなどのソフトウェアに依存しないで、セキュリティ対策を行うことが出来るようにする方法を明らかにするものである。IoT機器のセキュリティ対策として、CPUの内部情報を機械学習させることで、ハードウェアのみで異常検知を行う研究は他に無く、学術的にも新規性がある。また、ハードウェア実装することで、ワイヤースピードでの動作が可能となるため、高速に移動する物体などのリアルタイム処理を行う必要があるようなIoT機器でもセキュリティ対策が可能となることを証明できた。再学習可能とする方法も検討しており、社会実装の実現性も高いと考える。

研究成果の概要（英文）：1) The internal processor information effective for detecting abnormal CPU behavior includes the execution address, L1 instruction cache, and L1 data cache hit rates (overall, kernel space, and user space). 2) Random forests are suitable for implementing machine learning circuits on small hardware. 3) This function can be implemented with a small-scale circuit that does not affect the CPU implementation. 4) By reducing circuit scale and power consumption through bit width reduction and division tables without compromising features, it is possible to achieve these reductions without affecting the judgment results. 5) The hardware-implemented machine learning circuit can be retrained. 6) It was possible to actually operate on hardware equipped with a small-scale FPGA.

研究分野：ハードウェアセキュリティ

キーワード：ハードウェアセキュリティ　IoTセキュリティ　サイバーセキュリティ　異常動作検知　機械学習　RISC-V　マルウェア対策　プロセッサ

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

近年、本格的な IoT 時代が到来し、身の回りには数多くの IoT デバイスが存在するようになりました。2020 年には 400 億個を超えると予測されています［総務省平成 30 年版情報通信白書より］。IoT デバイスは組み込み機器と汎用的なコンピュータ双方の特徴を備えた新しいデバイスであり、具体的には次のような特徴を持ちます。

（１）汎用の民生部品やソフトウェアが多く使用されている

（２）ネットワーク接続などの機能を実現するため、高機能な OS や複雑な処理を行うアプリケーションが動作している

（３）メンテナンスされることなく長期間動作し続ける

（４）オフィスや家庭などで使用されているコンピュータよりも CPU やメモリ等のリソースが少ない

（５）インターネットに接続することが前提で、常にサイバー攻撃にさらされる

IoT デバイスは大量にネット接続されており、攻撃対象となることからセキュリティ対策は必須となっています。一方で、従来型の PC で導入されているウイルス対策ソフトのような、リアルタイムで通信を監視して攻撃を検知する動作などは、CPU による処理が多く電力消費が大きく、IoT デバイスのようにリソースに余裕がない場合は導入が困難です。そのため、従来とは異なる観点でのセキュリティ対策の検討が喫緊の課題となっています。

本研究は、IoT デバイスのような限られたリソース上でも最低限のセキュリティ対策機能を実現できるよう、正常もしくは異常動作を学習させ、プログラム動作の異常検知機能を CPU 自体に実装し、アンチウイルスなどのソフトに依存しない、セキュリティ対策を可能とすることを目指すものです。

２．研究の目的

上記の実現のために、（１）プログラムの動作に関連する、CPU 内部の特定情報を外部回路へ出力するプロセッサの機能開発、（２）目的（１）で出力される情報を元に、プログラムの正常動作、サイバー攻撃やマルウェア実行による異常動作を、適切に学習・分類する方法の調査研究、（３）目的（１）（２）それぞれの機能を、FPGA などを利用してハードウェア実装、これらを行います。実装の全体像を図１に示します。

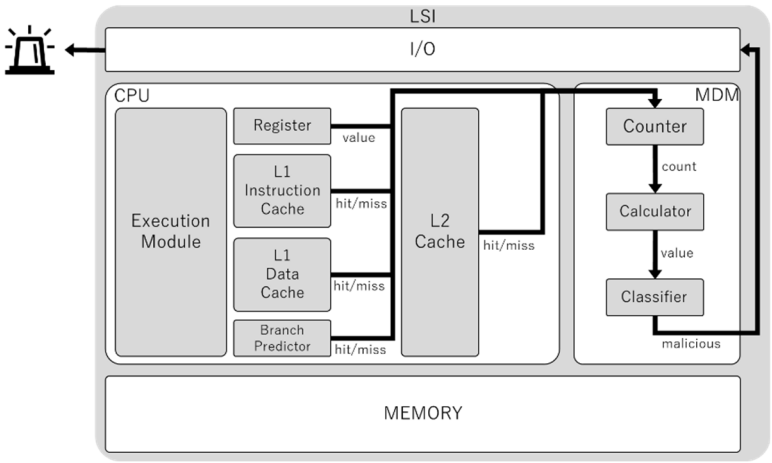

図１　実装全体像

３．研究の方法

（１）本来外部に出力されない CPU 内部の情報を得るためには、CPU 内部から直接信号を取り出す必要があります。市販の CPU では直接的に信号を取り出すことができない為、本研究では、FPGA 上で動作する RISC-V を CPU として利用します。具体的には、キャッシュヒット率など内部の信号を直接取り出すことができるよう、RISC-V のコードを修正し、外部回路に直接信号出力できるプロセッサを実装します。実装に当たっては、シミュレータを使用して HDL ベースでシミュレーションを行い、最終的に FPGA で動作させるものとします。

（２）本研究では、IoT 機器で使用する CPU を想定して異常動作検知機能を実装するため、回路規模が限られることが想定されます。機能を損なわないよう回路規模を小さくすることが必要となるため、異常動作判定に不要な信号や処理は出来る限り減らす必要があります。そこで、限られたリソースで効果的に異常判定が出来る信号を選定するために、CPU エミュレータを利用して様々な信号を取り出す仕組みを実装します。まず、CPU 内部の信号を記録するよう機能追加したエミュレータ上で良性プログラムと悪性プログラムを動作させ、それぞれのキャッシュヒット率や分岐予測情報などの情報（以下トレース情報と表記）を一命令ごとに取得します。次にトレース情報を学習させた各種の機械学習回路で実際に良性・悪性の検知ができるかどうかを検証します。検証の結果から、異常検知の寄与率が高い情報、および、小規模なハードウェア実装に適した機械学習方式を選別します。これらを合わせることにより、小規模な回路で適切に正常動作と異常動作を分類する方法を明らかにします。

（３）方法（２）で異常動作検知に対して寄与率の高い信号の特定、および、ハードウェア実装に適した機械学習方式の選択を行った後、方法（１）で開発する CPU と、トレース情報を学習した機械学習回路を結合し、FPGA 上に CPU として実装し、提案手法が有効に動作することを確認

します。

４．研究成果

本研究の成果として、以下の内容が明らかとなりました。

（１）CPU の異常動作検知に利用可能な CPU 内部情報

CPU から取得できる内部情報は１８種類存在しますが、評価の結果、寄与率が高い情報は限られることが分かりました。L2 キャッシュのヒット率、分岐予測情報などは寄与率が低く、加えて、小規模な IoT デバイスにはこれらの機能が搭載されていないことが考えられるため、内部情報として取得する必要がないと判断できます。具体的に、寄与率が高い変数は、アドレス情報、L1 命令キャッシュの全体ヒット率、カーネル空間ヒット率、ユーザ空間ヒット率、L1 データキャッシュの全体ヒット率、カーネル空間ヒット率、ユーザ空間ヒット率でした。

（２）CPU の異常動作検知に適した機械学習方式

これまでに得られている知見から、ニューラルネットのハードウェア実装は回路規模が大きくなる傾向があることから、ニューラルネットは使用しないことを前提とし、調査を行ったところランダムフォレストが小型のハードウェア実装に適していることが分かりました。ランダムフォレストを用いて動作しているプログラムの良性悪性判定を行ったところ、50%の閾値を設定することで、良性・悪性の判定を行うことが可能でした。

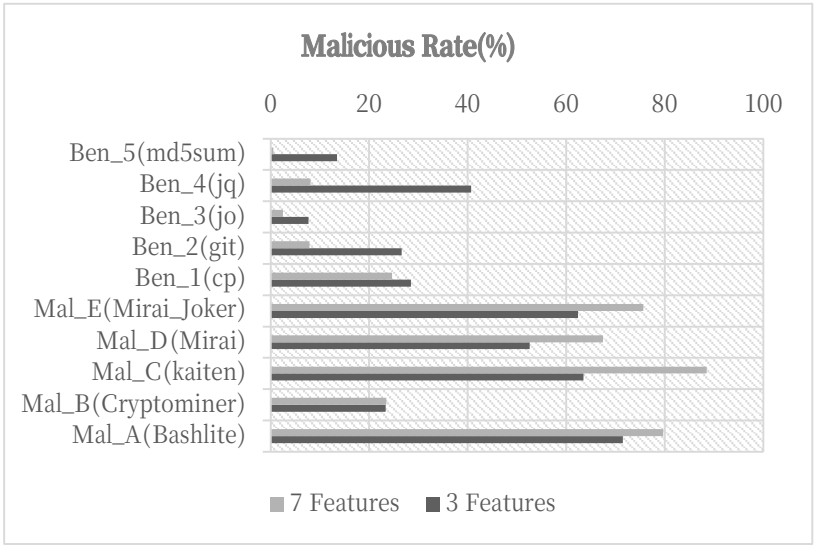

図２ 良性・悪性判定結果

（３）CPU の異常動作検知を行うための CPU と機械学習回路の接続方法

CPU のアーキテクチャとして RISC-V を使用し、コアのプログラムに手を加えることで、内部信号を直接取り出すことが可能となりました。機械学習回路との接続については、論理合成を行い、エミュレーションおよび実機で回路の連携動作が可能であることが確認できました。

（４）CPU に異常動作検知を行う回路を加えた場合の回路規模や消費電力の算出

CPU および機械学習回路を VerilogHDL で記述し、エミュレータ上で回路規模、および消費電力の測定を行いました。結果として、CPU 実装に影響を及ぼさない規模で本機能を実装可能なことが明らかとなり、また、機械学習回路の追加による電力の増加は微量にとどまることが分かり、実用困難な電力増加とならないことが明らかとなりました。

（５）異常動作検知を行う回路の小型化手法

研究開始当初において、機械学習に用いる変数の値として、キャッシュヒット率を用いていましたが、ヒット率を用いると、キャッシュヒットした命令数を全実行命令数で割り算する必要があります。この割り算は浮動小数点演算となるため、計算量やデータサイズが無視できないものとなります。しかし、提案手法では割り算の結果は１命令ごとに大きく変動しないため、下位ビットを切り捨てて桁上げし、整数演算を行うようにアルゴリズムの変更を行いました。さらに、先に割り算を行った結果を格納しておく「割り算表」を用意することで、動的に計算を行わないよう回路の修正を行い、判別精度を落とさず、回路規模の縮小、消費電力の削減が可能となりました。

（６）ハードウェア実装された機械学習回路を再学習させる方法

本研究では、機械学習にランダムフォレストを使用していますが、学習結果を即値でハードウェアに書き込むと、学習内容の更新が困難となります。また、VerilogHDL で記述された回路を論理合成する時点で最適化が行われてしまい、木構造が固定化されてしまうことがわかりました。そこで、回路上では完全な二分木を構成しつつ、判定に必要なパラメータを外部メモリに保持することで、学習内容の更新を行うことができる手法を考案しました。（特許出願中）

（７）プロトタイプ実装による提案手法の実現性

本研究で作成した RISC-V CPU と機械学習回路を論理合成し、小規模な FPGA を搭載したボード（Zync-7000）で実際に動作させることに成功しました。また、研究成果（６）等と合わせて、学習内容の更新が可能となることにより、実用上の課題となる回路規模、電力、学習内容の更新が解消できることが分かりました。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　3件）

１．著者名 Deguchi Mutsuki、Katoh Masahiko、Kobayashi Ryotaro	４．巻 12
２．論文標題 Evaluation of implementability in a malware detection mechanism using processor information	５．発行年 2022年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 253～269
掲載論文のDOI（デジタルオブジェクト識別子） 10.15803/ijnc.12.2_253	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Koike Kazuki、Kobayashi Ryotaro、Katoh Masahiko	４．巻 -
２．論文標題 IoT-oriented high-efficient anti-malware hardware focusing on time series metadata extractable from inside a processor core	５．発行年 2022年
３．雑誌名 International Journal of Information Security	６．最初と最後の頁 1,19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10207-021-00577-0	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Deguchi Mutsuki、Katoh Masahiko、Kobayashi Ryotaro	４．巻 13
２．論文標題 Low Resource and Power Consumption and Improved Classification Accuracy for IoT Implementation of a Malware Detection Mechanism using Processor Information	５．発行年 2023年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 149～172
掲載論文のDOI（デジタルオブジェクト識別子） 10.15803/ijnc.13.2_149	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　5件）

１．発表者名 Deguchi Mutsuki, Katoh Masahiko, Kobayashi Ryotaro
２．発表標題 Evaluation of low-cost operation of a malware detection mechanism using processor information targeting the IoT
３．学会等名 CANDAR 2022（国際学会）
４．発表年 2022年

１．発表者名
林壱成，加藤雅彦，小林良太郎

２．発表標題
プロセッサ情報を用いたマルウェア検知機構におけるバージョン互換性有無の評価

３．学会等名
コンピュータセキュリティシンポジウム2022(CSS2022)

４．発表年
2022年

１．発表者名
Deguchi Mutsuki、Katoh Masahiko、Kobayashi Ryotaro

２．発表標題
Evaluation of implementability in a malware detection mechanism using processor information

３．学会等名
CANDAR 2021（国際学会）

４．発表年
2021年

１．発表者名
出口睦樹,加藤雅彦,小林良太郎

２．発表標題
プロセッサ情報を用いたマルウェア検知機構のFPGA実装のための予備評価

３．学会等名
コンピュータセキュリティシンポジウム2020

４．発表年
2020年

１．発表者名
荻原拓海,小林良太郎,加藤雅彦

２．発表標題
ダミーファイルを用いた暗号化型ランサムウェアの検出と防御に関する検討

３．学会等名
コンピュータセキュリティシンポジウム2020

４．発表年
2020年

１．発表者名
山本真生,小林良太郎,加藤雅彦

２．発表標題
3D画像識別によるマルウェア検知を目的としたプログラムの挙動の可視化に関する検討

３．学会等名
第91回CSEC・第40回SPT・第90回EIP合同研究発表会

４．発表年
2021年

１．発表者名
荻原拓海,小林良太郎,加藤雅彦

２．発表標題
デコイファイルを用いた暗号化型ランサムウェアの検知とプロセス特定に関する検討

３．学会等名
第186回DPS・第92回CSEC合同研究発表会

４．発表年
2020年

１．発表者名
田中智也,小池一樹,小林良太郎,加藤雅彦

２．発表標題
ダミーファイルを利用した暗号化型ランサムウェア対策システムの実装

３．学会等名
コンピュータセキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
永井雄也,小林良太郎,加藤雅彦,嶋田創

２．発表標題
プロセッサ情報によるマルウェア検知における特徴量のビット数削減手法の検討

３．学会等名
コンピュータセキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
石川亮太,小林良太郎,加藤雅彦,嶋田創

２．発表標題
画像処理ベースのプログラム識別を目的としたプログラムの挙動の可視化に関する検討

３．学会等名
情報処理学会CSEC研究会

４．発表年
2019年

１．発表者名
K. Koike, R. Kobayashi and M. Katoh

２．発表標題
Reduction of Classifier Size and Acceleration of Classification Algorithm in Malware Detection Mechanism Using Processor Information

３．学会等名
2019 Seventh International Symposium on Computing and Networking Workshops（国際学会）

４．発表年
2019年

１．発表者名
Taku Sudo, Ryotaro Kobayashi, Masahiko Kato

２．発表標題
Single-Hardware Method to Detect Malicious Communications and Malware on Resource-Constrained IoT Devices

３．学会等名
CANDAR2023（国際学会）

４．発表年
2023年

１．発表者名
Yutaro Matunaka, Ryotaro Kobayashi, Masahiko Kato

２．発表標題
Verification of IoT Malware Match Rate Using Signatures Created Based on Processor Information

３．学会等名
CANDAR2023（国際学会）

４．発表年
2023年

１．発表者名 藤原京平，小林良太郎，加藤雅彦
２．発表標題 プロセッサ情報の平均特徴量および空間特徴量を用いた悪性通信を検出する機構の評価
３．学会等名 コンピュータセキュリティシンポジウム2023（CSS2023）
４．発表年 2023年

〔図書〕　計0件

〔出願〕　計3件

産業財産権の名称 検知回路	発明者 小林良太郎，加藤雅彦	権利者 工学院大学，長崎県立大学
産業財産権の種類、番号 特許、特願2023-52449	出願年 2022年	国内・外国の別 国内

産業財産権の名称 制御システム、及び制御回路	発明者 小林良太郎，加藤雅彦	権利者 工学院大学，長崎県立大学
産業財産権の種類、番号 特許、特願2023-52450	出願年 2022年	国内・外国の別 国内

産業財産権の名称 ハードウェアで実現された判別器の木構造を小規模な回路で更新可能とする技術	発明者 小林良太郎，加藤雅彦	権利者 工学院大学，長崎県立大学
産業財産権の種類、番号 特許、特願2023-221567	出願年 2023年	国内・外国の別 国内

〔取得〕　計0件

〔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	小林　良太郎 (Kobayashi Ryotaro) (40324454)	工学院大学・情報学部（情報工学部）・教授 (32613)	

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