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 ２２ 日現在

機関番号：３２６１３
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００００７６

研究課題名（和文）セキュリティアクセラレーションに対応した高効率なIoT向けメニーコア

研究課題名（英文）High efficiency IoT many-core for security acceleration

研究代表者
小林　良太郎（Kobayashi, Ryotaro）

工学院大学・情報学部（情報工学部）・教授

研究者番号：４０３２４４５４

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究では、セキュリティアクセラレーションに対応した高効率なIoT向けのメニーコアの開発を目的とする。研究期間において、細粒度の電力制御機構の開発を行った。開発した電力制御機構は動的電圧周波数制御が有効となっている時に、電力をさらに低減する機能を持つ。また、コアにセキュリティ機能をハードウェアとして付与することによって、高効率にセキュリティ対策を可能にする研究を行った。

研究成果の学術的意義や社会的意義
コンピュータは高速化や省電力化だけでなく、セキュリティの確保も必須となっている。しかし、年々深刻となるサイバー攻撃に対応するため、セキュリティ対策は速度低下や消費電力の増加をもたらしてしまう。それに対し、本研究成果は、パソコン利用者の利用状況に応じてコアの動作モードを細かく制御することを可能にした。また、従来ソフトウェアで実現されていたセキュリティ対策をハードで実現できるようにした。

研究成果の概要（英文）：In this research, we aim to develop a highly efficient many-core for IoT, which enables security acceleration. During the research period, we developed a fine-grained power control methods. The power control methods have the functions reducing power when enabling dynamic voltage frequency control. In addition, we also study the high efficiency security measures adding security functions implemented in hardware to the core.

研究分野：プロセッサ

キーワード：メニーコア　IoT　高効率

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

近年のプロセッサは、1 チップ上に多数のプロセッサコアを載せたメニーコアが主流である。メニーコアの用途は様々であるが、それらの１つである IoT デバイスは、2015 年に 49 億個存在しており、2020 年には 200 億個を超えると予測されている[Gartner 社の報告]。
IoT の主な特徴は、
(1)厳しいリソース制約を満たすために高効率なシステムが求められており、
(2)センサデータや制御データを扱うために OS の実行比率が高くなっており、
(3)IoT へのサイバー攻撃が急増している[Symantec 社の報告]ためにセキュリティ対策が必須となっていることにある。

２．研究の目的

そこで本研究では、汎用アプリ、OS、セキュリティ対策ソフトから成るプログラム群を高効率に実行する IoT 向けメニーコア・プロセッサを実現する。高効率な IoT 向けメニーコア(図 1)を実現するため、1 チップ上に電力の高い 64 ビットコアと電力の低い n ビットコア(n＜64)を集積し、プログラム毎、あるいは、プログラム内の命令ごとにデータのビット幅を動的に圧縮し、電力の低い n ビットコアでより多くの命令を処理する。

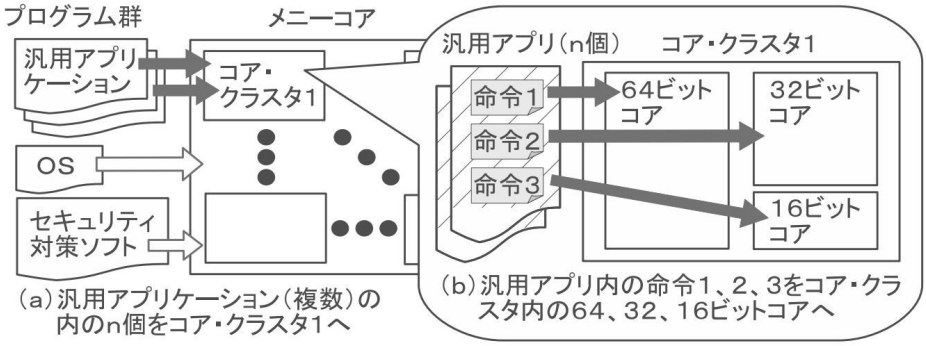

図1：高効率なIoT向けメニーコア

３．研究の方法

IoT 向けメニーコアの評価環境を構築し、低電力 n ビットコアの開発、命令をコアへと割り振るスケジューリング手法の開発を行う。その後、OS 側から n ビットコアの電力を制御するインターフェース(IF)の実装、プログラムをコア・クラスタへと割り振るスケジューリング手法の開発を行い、n ビットコア、および、コア・クラスタのチップ試作とメニーコア構成の設計を行う。

４．研究成果

増大するサイバー攻撃の脅威、および、IoT デバイスの急速な普及に対し、ハードウェアとソフトウェアの両面から以下 3 つに大別される研究を実施してきた。以下では、「５．主な発表論文等」に示した成果を[第１著者名.発表月.発表年]の形式で引用しつつ、研究成果を概説する。

【①マルウェア検出】コア内部の動作情報に基づく機械学習や深層学習によってマルウェアの検知が可能であることを示した研究[Tobiyama.Sep.2019, Takase.June.2019]、ストレージアクセスパターンを特徴量とした機械学習により、ランサムウェアを検出する研究[Hirano.Oct.2019]がある。上記[Takase.June.2019]の成果は、本研究のプロトタイプとして使用する。上記[Hirano.Oct.2019]の評価環境は、ストレージアクセスのログを蓄積し、効率的に検索するシステムを開発する研究の成果[Hirano.Oct.2018, Hirano.Dec.2017]によって実現されている。

【②悪性通信検出】DNS サーバへの DDoS 攻撃の一種である DNS Water Torture 攻撃に対し、ドメイン名のランダム性に着目して機械学習による悪性通信の検出とフィルタリングを同時に行うシステムの研究[Yoshida.Sep.2017]がある。[Yoshida.Sep.2017]では、ハードウェア(FPGA)によるアクセラレーションにより、オンラインでの高速なパケット処理を可能としている。さらに、攻撃に起因する悪性通信に対し、検知システム評価用のデータセットの研究[多田.9.2017]、機械学習ベースの悪性通信検知システム構築のための分散処理フレームワークの研究[多田.9.2019]を実施した。

【③IoT デバイス向け高効率プロセッサ】IoT デバイスは、高性能と省電力のバランスが良いプロセッサが求められる。この課題を解決するため、コア内部の特徴的な動作に着目し、キャッシュ[齋藤.3.2018]、データパス[Kobayashi.Dec.2017]等の省電力化を行うことによって、性能と電力のバランスに優れた高効率プロセッサを実現する研究を実施した。

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　8件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 多田竜之介，小林良太郎，嶋田創，高倉弘喜	４．巻 58
２．論文標題 NIDS評価用データセット：Kyoto 2016 Datasetの作成	５．発行年 2017年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1450-1463
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Takuro Yoshida, Kento Kawakami, Ryotaro Kobayashi, Masahiko Kato, Masayuki Okada, Hiroyuki Kishimoto	４．巻 25
２．論文標題 Detectiion and Filtering System for DNS Water Torture Attacks Relying Only on Domain Name Information	５．発行年 2017年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 854-865
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.25.854	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Manabu Hirano, Natsuki Tsuzuki, Seishiro Ikeda, Ryotaro Kobayashi	４．巻 7
２．論文標題 LogDrive: a Proactive Data Collection and Analysis Framework for Time-Traveling Forensic Investigation in IaaS Cloud Environments	５．発行年 2018年
３．雑誌名 Journal of Cloud Computing: Advances, Systems and Applications	６．最初と最後の頁 1-25
掲載論文のDOI（デジタルオブジェクト識別子） s13677-018-0119-2	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 多田竜之介，中村純哉，大村廉，小林良太郎	４．巻 60
２．論文標題 機械学習ベースNIDS構築のための分散処理フレームワーク	５．発行年 2019年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1448-1465
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名	4．巻
S. Tobiyama, Y. Yamaguchi, H. Hasegawa, H. Shimada, M. Akiyama, and T. Yagi	60
2．論文標題	5．発行年
Using Seq2Seq Model to Detect Infection Focusing on Behavioral Features of Processes	2019年
3．雑誌名	6．最初と最後の頁
JIP	545-554
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
なし	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	－

1．著者名	4．巻
Hayate Takase, Ryotaro Kobayashi, Masahiko Kato, and Ren Ohmura	-
2．論文標題	5．発行年
A Prototype Implementation and Evaluation of the Malware Detection Mechanism for IoT Devices using the Processor Information	2019年
3．雑誌名	6．最初と最後の頁
International Journal of Information Security	1,11
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1007/s10207-019-00437-y	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	－

1．著者名	4．巻
齋藤 郁, 小林 良太郎, 嶋田 創	59
2．論文標題	5．発行年
DVFS使用下における余剰時間を利用した最上位キャッシュ切替えによるキャッシュ消費エネルギーの削減	2018年
3．雑誌名	6．最初と最後の頁
情報処理学会論文誌	1061-1076
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
なし	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	－

1．著者名	4．巻
Ryotaro Kobayashi, Anri Suzuki, Hajime Shimada	7
2．論文標題	5．発行年
Forwarding Path Limitation and Instruction Allocation for In-Order Processor with ALU Cascading	2017年
3．雑誌名	6．最初と最後の頁
Journal of Low Power Electronics and Applications	-
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.3390/jlpea7040032	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	－

〔学会発表〕　計13件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 M. Hirano and R. Kobayashi
２．発表標題 Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained from Live-forensic Hypervisor
３．学会等名 IOTSMS 2019（国際学会）
４．発表年 2019年

１．発表者名 M. Hirano, T. Tsuzuki, S. Ikeda, N. Taka, K. Fujiwara and R. Kobayashi
２．発表標題 WaybackVisor: Hypervisor-based Scalable Live Forensic Architecture for Timeline Analysis
３．学会等名 TSP 2017（国際学会）
４．発表年 2017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	嶋田　創 (Shimada Hajime) (60377851)	名古屋大学・情報基盤センター・准教授 (13901)	