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 ２１ 日現在

機関番号：３２６１３
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１１８１８

研究課題名（和文）コア内部の動作情報を特徴量としてサイバー攻撃の検知を行うIoT向けプロセッサ

研究課題名（英文）IoT processor detecting cyber-attacks using operation information inside core as features

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）　　3,300,000円

研究成果の概要（和文）：IoT向けプロセッサによる不正アクセス対策の研究により、機械学習のアルゴリズムを使うことで高い精度の検知が可能になりました。また、デコイファイルを用いた研究により、低負荷かつ高精度なランサムウェアの検知が可能であることが示されました。これらの成果は、IoT向けのマルウェア対策の強化に大きく貢献しています。

さらに、IoT向けのマルウェア対策に、ハードウェア実装された判別器をLSI上のコアに隣接させました。プログラム実行中に、1命令ごとに悪性か良性かを判定して、最終判定を行います。この研究では、IoT機器に必要な判別器をより省スペースで、消費電力を削減する提案をしました。

研究成果の学術的意義や社会的意義
マルウェア対策の研究では、機械学習を使うことで高精度な検知が可能になり、デコイファイルによって低負荷かつ高精度なランサムウェア検知が可能となりました。これらの成果は、IoT機器への攻撃の脅威が高まる中で、プロセッサによる攻撃検知の重要性を示すものであり、IoT機器のセキュリティ強化に貢献すると言えます。更にLSI上のコアに隣接したハードウェア判別器は、IoTセキュリティにおける重要な一歩となり、今後も注目されることでしょう。IoTセキュリティの課題は多岐にわたり、今後も重要性が高まっていくと予想されます。

研究成果の概要（英文）：Research on countermeasures against unauthorized access using IoT processors has made it possible to achieve high-precision detection by using machine learning algorithms. In addition, research using decoy files has shown that it is possible to detect ransomware with low load and high accuracy. These achievements have greatly contributed to strengthening malware countermeasures for IoT.

Furthermore, for malware countermeasures for IoT, a hardware-implemented discriminator was placed adjacent to the core on the LSI. During program execution, it judges whether each instruction is malicious or benign, and makes a final judgment. In this research, a proposal was made to reduce the required space and power consumption of the necessary discriminator for IoT devices.

研究分野：サイバーセキュリティ

キーワード：サイバーセキュリティ

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年、IoT デバイスは急速に普及しており、生命・財産への関わりが更に増していきます。しかし、一方で、IoT デバイスへのサイバー攻撃が深刻化しています。2016 年には、米 Dyn 社への DDoS 攻撃がマルウェアの一種である Mirai によって発生し、同時期に Mirai のソースコードが GitHub で公開されたことが契機となり、IoT へのサイバー攻撃は激化しています。そのため、IoT のセキュリティ対策は必須となっています。

しかし、汎用 PC で用いられている既存手法を IoT 機器に導入することは難しいです。既存手法は、ソフトウェアとしての実装や定期的な更新を前提とするものがほとんどであり、十分なハードウェアリソース(CPU やメモリ等)、および、ベンダやユーザによる適切なメンテナンスを要求するため、多くの IoT 機器はリソース制約が厳しく、一旦設置されるとベンダやユーザのメンテナンスなしで長期間稼働することが求められます。これらより、既存のセキュリティ対策ソフトの導入は困難になっています。しかし、未だ根本的な対策が行われないまま、IoT 機器は急速に増加し続けており、生命・財産への関りが深い分野での高成長も予測されています。

２．研究の目的

本研究は、IoT 向けプロセッサによるサイバー攻撃の検知を目的としており、機械学習ベースの超軽量識別器を使用して、プログラム実行時に得られる動作情報を特徴量として抽出し、当該識別器を使用してサイバー攻撃による異常動作を検知することができます。これにより、高速かつ軽量でメンテナンスフリーな攻撃検知が可能となります。

３．研究の方法

本研究では、提案機構を搭載した IoT 向けプロセッサのエミュレーション環境において、コア内部の動作情報から特徴量を生成する手法の開発、生成した特徴量を元に、プログラムの正常動作、デーモンプログラムやマルウェアによる異常動作を、高い精度で学習・分類する手法の開発を行いました。また、提案機構のハードウェア実装のため、「抽出回路」と「超軽量識別器」を低コストで実現する手法の開発を行い、CAD や FPGA などを利用して、提案機構を備えたプロセッサのハードウェアによる実装と検証を行いました。これらの研究は、IoT 向けプロセッサによるサイバー攻撃の検知に関する知見を提供しています。

IoT セキュリティに関する課題は多岐にわたり、今後も研究の重要性が高まっていくことが予想されます。報告書にまとめた研究成果は、IoT 機器のセキュリティ強化に貢献するものと言えます。今後も、IoT 機器に対する攻撃の脅威に対して、IoT 向けプロセッサによる高度な攻撃検知技術の開発が求められます。

４．研究成果

本文書は、IoT 向けプロセッサによるサイバー攻撃の検知を目的とした 3 つの研究実績について報告しています。IoT 機器は近年、急速に普及しており、その利便性が増す一方で、セキュリティリスクも高まっています。IoT 向けプロセッサによる攻撃検知技術は、IoT 機器のセキュリティを強化するために必要不可欠な技術となります。

1 つ目の研究実績は、不正アクセス対策に焦点を当てたものです。不正アクセスは、近年急増しており、IoT 機器に対する脅威となっています。研究では、悪性通信と正常通信を発生させる機構を設置し、発生させた通信から定期的に判別器を生成・更新し、より適切なアルゴリズムを動的に選択する研究を実施しました。これにより、IoT 機器に対する不正アクセスに対する高精度な検知が可能となりました。

2 つ目の研究実績は、ランサムウェア対策に焦点を当てたものです。ランサムウェアは、データを暗号化し、解除キーを要求することで、被害者から身代金を要求する悪質なマルウェアです。この研究では、ランサムウェア用にデコイファイルを用意し、まずデコイファイルを直接監視することによって、ランサムウェアが暗号化を行っているという動作を間接的に検知し、つぎに各プロセスのファイル操作を監視することによって、デコイファイルの暗号化を行っているプロセスを特定する研究を行いました。この研究では、低負荷で高精度な検知技術を開発し、IoT 機器のセキュリティ強化に貢献しました。

3 つ目の研究実績は、IoT 向けのマルウェア対策に焦点を当てたものです。IoT 機器において、

マルウェアによる攻撃は深刻な問題となっています。この研究では、LSI 上のコアと隣接する位置にすべてハードウェア実装された判別器を用意し、プロセッサ情報を特徴量として、プログラムを実行しながら、悪性か良性かの判定を行う研究を実施しました。この研究では、IoT 機器で必要とされる判別器のハードウェア量削減と消費電力削減を実現することができる手法を提案し、実際に FPGA 上をターゲットとして実装することによって、その効果を定量的に示しました。

これらの研究実績により、IoT 向けプロセッサによるサイバー攻撃の検知技術に関する知見が得られ、IoT 機器に対するセキュリティリスクの低減に貢献することができました。今後も、IoT 機器に対する攻撃の脅威に対して、IoT 向けプロセッサによる高度な攻撃検知技術の開発が求められます。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1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 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 -
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 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Hideya Sato, Ryotaro Kobayashi
２．発表標題 A machine learning-based NIDS that collects training data from within the organization and updates the discriminator periodically and automatically
３．学会等名 The 8th International Workshop on Information and Communication Security (WICS 2021)（国際学会）
４．発表年 2021年

１．発表者名 荻原拓海，加藤雅彦，小林良太郎
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 佐藤秀哉，林はるか，小林良太郎
２．発表標題 組織内ネットワークにおけるハニーポットを備えた動的な機械学習ベースのNIDSの作成と予備的評価
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
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
情報処理学会CSEC研究発表会

４．発表年
2020年

１．発表者名
林はるか，佐藤秀哉，小林良太郎

２．発表標題
機械学習ベースのNIDSにおける動的な判別器生成に関する検討と予備評価

３．学会等名
情報処理学会CSEC研究発表会

４．発表年
2020年

１．発表者名
佐藤秀哉，林はるか，小林良太郎

２．発表標題
組織内で学習データを採取し定期的に判別器を更新する機械学習ベースのNIDS

３．学会等名
情報処理学会CSEC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
情報処理学会CSEC研究発表会

４．発表年
2021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)	

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