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　　元 年　　６ 月 １９ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００００７１

研究課題名（和文）対サイバー攻撃アルゴリズムのスループットと電力性能比を向上する計算機システム

研究課題名（英文）Computer system which improves both throughput and power performance ratio for counter cyber attack algorithmsh

研究代表者
嶋田　創（Shimada, Hajime）

名古屋大学・情報基盤センター・准教授

研究者番号：６０３７７８５１

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）：プロセッサ・アーキテクチャにおける電力性能比を改善する研究として、特に、超低消費電力志向プロセッサにおけるDVFS下での余剰時間利用による高速/低速最上位キャッシュ切り替え利用、および、ALUカスケーディングを行う3命令発行イン・オーダ実行プロセッサにおけるフォワーディング・パス制限において高い成果をあげた。対サイバー攻撃アルゴリズムの研究において、特に、APIコール・ログの多段DNN処理によるマルウェア・プロセス判別、および、リクエスト間隔とレスポンス・サイズによるマルウェア感染由来のHTTP/HTTPS通信検知において高い成果をあげた。

研究成果の学術的意義や社会的意義
学術的な意義が評価された研究成果として、APIコール・ログ利用のマルウェア検知における2段階DNN利用の検知アルゴリズムがある。この研究はICOIN2018 Best Paper AwardとCSS2017奨励賞の授与を受けた。また、社会的な意義も強い研究成果として、NIDSの攻撃検知研究向けにIDS検知結果を付与した10年分のハニーポットの観測データをKyoto 2016 Datasetとして整備するとともに、機械学習系攻撃検知における検知結果の変化についてまとめた論文が、本研究成果はIPSJ 論文誌ジャーナル/JIP特選論文として選ばれた。

研究成果の概要（英文）：As in power performance improvement researches on processor architecture area, we achieved good results on 2 researches. The one is switching low/high speed highest-level caches under DVFS for super low power processors and the other one is forwarding path limitation for 3-way in-order ALU cascading processor.
As in counter cyber attack algorithm research area, we achieved good results on 2 researches. The one is malware process estimation with processing API call log with multi-stage DNN and the other one is malware originated HTTP/HTTPS traffic detection with clustering based on request interval and response size.

研究分野：情報セキュリティ

キーワード：計算機アーキテクチャ　情報セキュリティ　ネットワークセキュリティ　マルウェア検知/分類

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

近年では様々なサイバー攻撃が脅威となっており、様々なサイバー攻撃検知手法が研究において提案されている。しかしながら、それらの研究の多くは検知率向上に注力しており、検知手法の処理速度の向上への注力は少ない。特に、近年注目されているアノマリ検知では、従来のシグネチャ型検知と比較して計算量が増えるため、処理速度の向上が必要となる。一方、監視対象となる通信トラフィックにおいては、インターネット・トラフィックは年率 23%の増加を続けると予測されていると同時に、近年の標的型攻撃対策のためにイントラネットの監視の重要性が増しており、インターネット・トラフィックよりも 1 桁上の通信の監視の必要性も出ている。また、近年では組み込みシステムへのサイバー攻撃が増加しており、電池寿命や発熱の点から電力制約の厳しいシステムにおいてサイバー攻撃対策技術を導入する必要性が増している。すでにサイバーセキュリティはコスト対効果も含めて実施する段階にあり、悪性トラフィック検知やマルウェア検知においても電力効率の向上の視点も含めたアルゴリズム開発や実装が必要であると考える。

２．研究の目的

すでにサイバーセキュリティはコスト対効果も含めて実施する段階にあり、悪性トラフィック検知やマルウェア検知においても電力効率の向上の視点も含めたアルゴリズム開発や実装が必要であると考える。本研究では、悪性ネットワーク・トラフィック検知やマルウェア検知を対象とした､対サイバー攻撃関係のアルゴリズムの電力効率の向上を目標とする｡これにより、スループットの向上により、PC クライアントにおける防衛において負荷を低減させてユーザの利便性を向上させると同時に、従来からの課題である、検出の高精度化とリアルタイム性の維持も行う。また、電力性能比向上により、サイバー攻撃対策で消費される電力を削減することで環境負荷軽減に貢献するとととともに、組み込み機器など、従来では電力制約が厳しくて対策を実施できなかった機器に対して、防衛手段を与えることを実現する。

３．研究の方法

対サイバー攻撃アルゴリズムの電力性能比は以下の方針で実施する。

1. 同程度の計算量で高い検知精度を達成するアルゴリズムの開発
2. あるアルゴリズムにおいて計算量あたりの検知精度向上が悪くなる領域を使うのをあきらめ、浮いた計算資源で他のアルゴリズムを利用する
3. GPGPU や FPGA を利用して計算に用いるビット数を削減した低精度演算を実装し、1 演算あたりの電力効率を上げるなど、プロセッサ・アーキテクチャの改良を伴う電力性能比向上

未知攻撃検出、マルウェア分類の研究経験がある名古屋大学グループと、メニーコアを用いた 1 プログラムの実行の高速化とサービス不能攻撃防御の研究経験がある豊橋技科大グループで研究組織を組織した。

４．研究成果

プロセッサ・アーキテクチャの改良を伴う電力性能比向上として雑誌論文および国際会議で発表を行った以下の 2 点について特に説明する。

(1) DVFS 下での余剰時間利用による高速/低速最上位キャッシュ切り替え利用[J1, P24]

IoT デバイス等に搭載される超低消費電力志向のプロセッサにおいては、プロセッサに内包するキャッシュ・メモリの消費電力の割合が相対的に大きくなる。これは、キャッシュを構成する SRAM は値を保持する 4 個の FET の電流駆動能力がばらつくと正常に動作しないため､低消費電力化で第 1 に利用される電源電圧低下(FET の電流駆動能力のばらつきが相対的に大きくなる)させて動作させることが難しいためである。プロセッサ・コアについては、処理の負荷が軽い時に電源電圧と周波数を低下させる動的電源周波数制御(DVFS)制御が多用されているが、キャッシュについてはクロック周波数低下時においても電源電圧を下げづらい状況にある。低電圧動作耐性を持たせるために、ゲート長の延長等のデバイスレベルでの対応を取ることは可能だが、その対策は高速動作の相反するもののため、特に速度が要求される最上位キャッシュには使いづらい。そのため、低負荷時の低クロック動作時には、最上位キャッシュには動作クロックに対して必要以上に高い電源電圧が供給される状態となる。

近年では、半導体製造技術の微細化によって FET が高密度に詰め込まれ、それらの FET を同時に動作すると電力密度や熱密度の問題が発生することが懸念されており、ダーク・シリコン問題と呼ばれ、同時に動かせない余ったシリコンを活用する動きとなっている。この問題はいずれ、放熱機構や電源部に制約が出る IoT デバイスでも問題になることが想定され、そのような用途で用いられる超低消費電力志向プロセッサでもダーク・シリコン活用の問題は出てくると考える。

そこで、本研究では最上位キャッシュを高速/高消費電力/低電源電圧動作に難があるキャッシュ(LOHS キャッシュ)と低速/低消費電力/低電圧耐性ありのキャッシュ(LOLS キャッシュ)を 2 種類実装し、DVFS 下において切り替え動作させることを提案する。提案では単に切り替え動作を行うのみならず､LOLS キャッシュでも余裕時間が発生する超低クロック動作時には LOHS と LOLS のシーケンシャルアクセスを行うことで実効的なキャッシュ容量を増大させ､消費エネルギーを削減する。評価の結果、提案は SPECint2006 ベンチマーク実行において最大 23.5%、

SPECfp2006 ベンチマーク実行において最大 27.2%の消費エネルギー削減が実現できることを確認した。

(2) ALU カスケーディングにおけるフォワーディング・パス制限[J2, P23]

回路面積あたりの性能および電力性能比の観点から、メニーコア・プロセッサにおいては 2 命令程度のイン・オーダ実行のプロセッサ・コアが用いられる事例が多い。これは、アウト・オブ・オーダ実行に必要となる命令ウィンドウやリオーダ・バッファは全エントリが均等に高速動作することを求められるため、クリティカル・パス以外を低速/低消費電力トランジスタで構成するような技術を用いることが難しく、得られる性能向上に対して電力性能比が悪化するためであるとともに、回路面積上でも不利なためである。一方で、イン・オーダ実行は 3 命令以上の同時実行についてはデータ依存の観点から意義がほぼ無く、3 命令以上の同時実行についてはアウト・オブ・オーダ実行が必須となる。しかしながら、メニーコア・プロセッサでは熱密度や電力密度の問題から全コアが FET の動作の上限で動いていることはなく、DVFS による動作クロック周波数低下時においても、例えば演算器の部分においても演算終了後に余裕時間が発生している。過去の提案でこの余裕時間を利用してデータ依存関係にある別命令を実行する ALU カスケーディングを伴う 3 命令以上のイン・オーダ実行を提案した。本研究はこの ALU カスケーディングを伴う 3 命令実行イン・オーダ実行プロセッサの改良の提案である。

本研究では、プロセッサ回路において一般的にクリティカル・パスの 1 つとなるデータ・フォワーディングのパスにおいて、ALU カスケーディング用のパスを削減し、代わりに、時間的余裕のあるデコード・ステージにおいて命令並び替えを行うものである。これにより、特定のデータ依存関係のある命令間で ALU カスケーディングを行えなくなり IPC が低下が、回路面積や回路遅延を削減することで IPC の低下を補う。評価の結果、実行ステージ回りにおいて 38.7%の回路面積削減、23.2%の回路遅延を削減し、41.1%の消費エネルギー削減を実現できることを確認した。

また、対サイバー攻撃アルゴリズムに関する研究成果の代表として国際会議で発表を行った、以下の 2 点について特に説明する。

(3) API コール・ログの多段 DNN 処理によるマルウェア・プロセス判別[P12, P14, P21, P25]

近年の標的型攻撃では、攻撃者は既存のマルウェア検知機構で見つからないことを確認したマルウェアを作成した上で送り込むことが多く、そのようなマルウェアをいち早く見つけ出すことが重要となっている。そのため、本研究では、端末の上で動作中のプロセスのうち、マルウェアらしき挙動を占めすプロセスを提示することを目的とした。提案では、マルウェアらしきプロセスを探す端末上で全プロセスの API コール・ログを取得し、プロセスごとの API コール・ログからマルウェアらしき特徴量を持つものを提示する。

本研究では、API コール・ログの特徴量の圧縮に 1 段目の DNN、学習用のマルウェア/正常プロセスの圧縮された API コール特徴量を学習し評価用プロセスの判別を行う 2 段目の DNN を利用することで、高い検知率(TPR: True Positive Rate)と低い誤検知率(FPR: False Positive Rate)を達成した。多段利用する DNN については、1 段目に RNN および 2 段目に CNN を利用する構成、および、1 段目に seq2seq モデルおよび 2 段目に別の seq2seq モデルを利用する実装(図 1)を評価した。マルウェアから取得した API コール・ログと通常プロセスから取得した API コール・ログを用いて 5 分割交差検証を実施した結果、TPR と FPR からなる Area Under Curve の評価において前者は 0.970、後者は 0.979 の値を達成した。

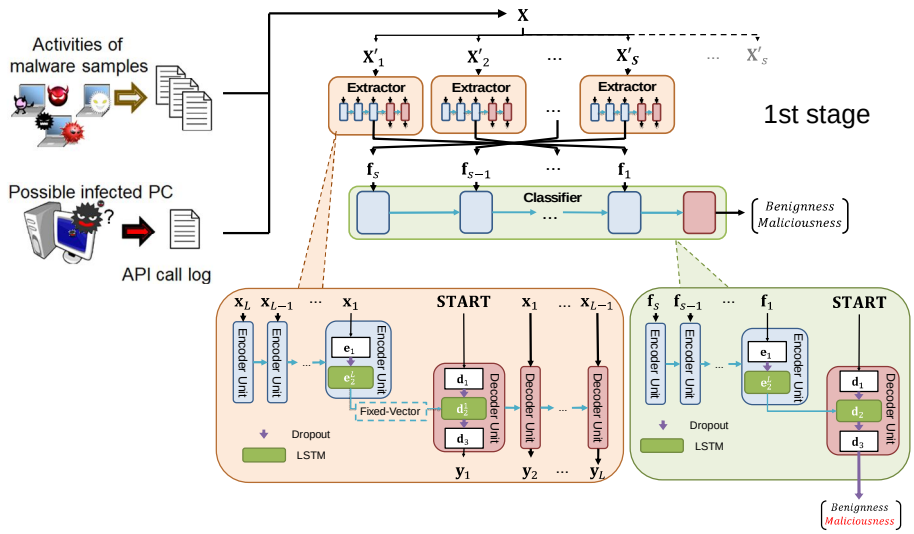

図 1: seq2seq モデルの 2 段人用によるマルウェア・プロセス判別

(4) リクエスト間隔とレスポンス・サイズによるマルウェア感染由来の HTTP/HTTPS 通信検知[P17, P20]

近年のサイバー攻撃では、感染した端末を遠隔操作してさらなる感染拡大の拠点とする Remote Administration Trojan(RAT)型のマルウェアが多用される。RAT は Command and

Control(C&C)サーバから遠隔操作司令を受け取って動作を行う。C&C サーバとの通信は、過去には IRC や独自プロトコルなどの比較的検知しやすいプロトコルを利用していたが、近年のマルウェアでは検知を逃れるために HTTP/HTTPS などの広く利用されているプロトコルを利用するものも現れ、中には、SNS のメッセージング機能を C&C 通信に利用する物まで存在する。

本研究では。RAT も含めたマルウェア感染由来の HTTP/HTTPS 通信を検知するため、HTTP/HTTPS 通信をリクエストとレスポンスのペア(図 2)に分類した上で、通信サイズや通信間隔などとともに特徴量を構成してクラスタリングを行い、教師あり SVM にてクラスタ分類を行った。マルウェア通信と平常時のネットワーク・トラフィックを利用して 5 分割交差検証を行った結果、F 値による評価で 0.986 という結果を得た。

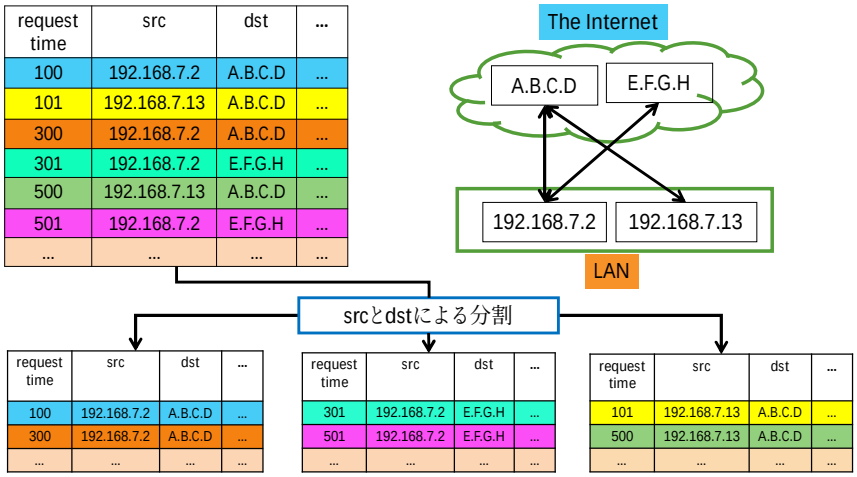

図 2: HTTP リクエスト/レスポンスペアへの分割

本研究課題に関連して、ネットワーク・トラフィックからの悪性通信検知のためのデータセットを整備しつつ過去からの検知精度の変化をまとめた物を公開したものに対して高い評価を受けた。

(5) NIDS 評価用データセット Kyoto 2016 Dataset 作成と統計調査[J3]

サイバー攻撃に対する防御方法として NIDS による攻撃検知があり、様々な研究が行われている。この NIDS による攻撃検知研究実施における障害として、評価に用いるデータセットの準備がある。データセットには検知対象とするカテゴリの攻撃が多数含まれているのが望ましいが、収集期間の短いデータセットでは攻撃のトレンド等によって、検知対象とする攻撃が少ないなどの問題が起こりうる。そのため、最新の攻撃傾向も含めつつ長期の攻撃記録を含めたデータセットである Kyoto 2016 Dataset を作成した上、そこに含まれる攻撃の統計情報、および、様々な期間において基本的な機械学習による攻撃検知を試みた結果をまとめ、今後の NIDS による攻撃検知研究を行う者が指標として利用できるようにした。

５．主な発表論文等

〔雑誌論文〕（計　6　件）

[J1] 齋藤郁，小林良太郎，嶋田創，"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，" 情報処理学会論文誌，Vol. 59，No. 3，pp. 1061-1076，2018 年 3 月.(査読有)

[J2] Ryotaro Kobayashi, Anri Suzuki, and Hajime Shimada, "Forwarding Path Limitation and Instruction Allocation for In-Order Processor with ALU Cascading," Journal of Low Power Electronics and Applications, Vol. 7, No. 4, pp. 1-15, DOI: 10.3390/jlpea7040032, December 2017. (査読有)

[J3] 多田竜之介，小林良太郎，嶋田創，高倉弘喜 "NIDS 評価用データセット : Kyoto 2016 Dataset の作成，" 情報処理学会論文誌 Journal of Information Processing. Vol. 58，No. 9，pp. 1450-1463，2017 年 9 月. (査読有)

[J4] 長谷川皓一，山口由紀子，嶋田創，高倉弘喜，"ディレクトリサービス情報とトラフィックデータによる ACL 自動生成システム，" 電子情報通信学会論文誌，Vol. J100-D，No. 3，pp. 353-364，DOI: 10.14923/transinfj.2016PDP0023，2017 年 3 月. (査読有)

[J5] Ryotaro Kobayashi, Ikumi Kaneko, and Hajime Shimada, "Improvement of Data Utilization Efficiency for Cache Memory by Compressing Frequent Bit Sequences," IEICE Transactions on Electronics, Vol. E99-C, No. 8, pp. 936-946, DOI: 10.1587/transele.E99.C.936, August 2016. (査読有)

[J6] Ryotaro Kobayashi, Kaoru Saito, and Hajime Shimada, "Energy Reduction of BTB by focusing on Number of Branches per Cache Line," Journal of Information Processing, Vol. 24, No. 3, pp. 492-503, DOI: 10.2197/ipsjjip.24.492, May 2016. (査読有)

〔学会発表〕(計 26 件)

[P1] 嶋田創, "事業継続とセキュリティインシデント封じ込めを両立させる情報システム構築," 電子情報通信学会 信頼性研究会 招待講演, 2019 年 2 月. (査読無)

[P2] 伊藤克恭, 長谷川皓一, 山口由紀子, 嶋田創, "Android 向け PUA と正規アプリ間の API 使用傾向の比較調査," 情報処理学会研究報告, Vol. 2018-CSEC-83, No. 18, pp. 1-6, 大分県別府市, 2018 年 12 月. (査読無)

[P3] 大橋宗治, 長谷川皓一, 山口由紀子, 嶋田創, "組織における標的型攻撃に対する挙動分析システムの提案(WIP セッション)," 第 11 回インターネットと運用技術シンポジウム (IOTS2018), p. 42, 鳥取県米子市, 2018 年 12 月. (査読無)

[P4] 張紫薇, 長谷川皓一, 山口由紀子, 嶋田創, "無線 LAN 環境における遅延ゆらぎに着目した不正アクセスポイントの検知の初期検討(WIP セッション)," 第 11 回インターネットと運用技術シンポジウム(IOTS2018), p. 43, 鳥取県米子市, 2018 年 12 月. (査読無)

[P5] Katsutaka Ito, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada, "Detecting Privacy Information Abuse by Android Apps from API Call Logs," In proceedings of the 13rd International Workshop on Security (IWSEC 2018), LNCS 11049, pp. 143-157, Sendai / Japan, September 2018. (査読有)

[P6] Seiya Takagi, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada, "Countermeasure for DNS Server Address Spoofing Attack by DHCPv6 Implementation Difference," In Proceedings of International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC2018), pp. 440-443, Bangkok / Thailand, July 2018. (査読有)

[P7] Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, and Hiroki Takakura, "A Countermeasure Recommendation System for Indicating Residual Risks (Poster)," In Proceedings of International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC2018), pp. 856-859, Bangkok / Thailand, July 2018. (査読有)

[P8] 坂梨元軌, 嶋田創, "攻撃対策を目的とした軽量プロトコル MQTT を利用した C&C ネットワークの評価," 情報処理学会第 80 回全国大会予稿集, 2W-02, pp. 479-480, 東京都新宿区, 2018 年 3 月. (査読無)

[P9] 高木聖也, 長谷川皓一, 山口由紀子, 嶋田創, "DHCPv6 クライアントの実装差を利用した DNS サーバアドレス詐称攻撃," 情報処理学会第 80 回全国大会予稿集, 2W-03, pp. 481-482, 東京都新宿区, 2018 年 3 月. (査読無)

[P10] 大橋宗治, 長谷川皓一, 山口由紀子, 嶋田創, "ハニーポットへの攻撃に対する NIDS 検知反応を利用したシグネチャの自動チューニング," 情報処理学会第 80 回全国大会予稿集, 2W-09, pp. 493-494, 東京都新宿区, 2018 年 3 月. (査読無)

[P11] Paul Calderon, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada, "Malware Detection Based on HTTPS Characteristic via Machine Learning (poster)," In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), pp. 410-417, Funchal / Portugal, January 2018. (査読有)

[P12] Shun Tobiyama, Yukiko Yamaguchi, Hirokazu Hasegawa, Hajime Shimada, Mitsuaki Akiyama, and Takeshi Yagi, "A Method for Estimating Process Maliciousness with Seq2Seq Model (Best Paper Award)," In Proceedings of the 32nd International Conference on Information Networking (ICOIN2018), pp. 255-260, Chiang Mai / Thailand, January 2018. (査読有)

[P13] Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada, "Mining for Operation Specific Actionable Cyber Threat Intelligence in Publicly Available Information Source," 暗号と情報セキュリティシンポジウム SCIS2018, 3F1-1, pp. 1-8, 新潟県新潟市, 2018 年 1 月. (査読有)

[P14] 飛山駿, 山口由紀子, 長谷川皓一, 嶋田創, 秋山満昭, 八木毅, "Seq2Seq モデルを用いたプロセスの悪性度推定手法(CSS2017 奨励賞)," コンピュータセキュリティシンポジウム 2017, pp. 1389-1396, 山形県山形市, 2017 年 10 月. (査読無)

[P15] 鍛治秀伍, 小林良太郎, 嶋田創, "アノマリ検知のための GPU を用いた One Class SVM の高速化," 電子情報通信学会総合大会, D-19-6, p.132, 愛知県名古屋市, 2017 年 3 月.

[P16] 小川秀貴, 山口由紀子, 嶋田創, 高倉弘喜, 秋山満昭, 八木毅, "DBSCAN によるクラスタ出現確率を用いたマルウェア感染由来の HTTP トラフィック検知," 情報処理学会第 79 回全国大会予稿集, 4W-03, pp. 585-586, 愛知県名古屋市, 2017 年 3 月. (査読無)

[P17] Hideki Ogawa, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, Mitsuaki Akiyama, and Takeshi Yagi, "Malware Originated HTTP Traffic Detection Utilizing Cluster Appearance Ratio," In Proceedings of the 31st International Conference on Information Networking (ICOIN2017), pp. 248-253, Da Nang / Vietnam, January 2017. (査読有)

[P18] Shohei Hiruta, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, Takeshi Yagi, and Mitsuaki Akiyama, "Evaluation on Malware Classification by Session Sequence of

Common Protocols," In proceedings of 15th International Conference on Cryptology and Network Security (CANS 2016), pp. 521-531, DOI: 10.1007/978-3-319-48965-0_31, Milano / Italy, November 2016. (査読有)
[P19] 多田竜之介, 小林良太郎, 嶋田創, 高倉弘喜, "新 Kyoto 2006+データセットの作成に関する検討と評価," 電子情報学会技術報告, Vol. 116, No. 328, ICSS2016-42, pp. 21-26, 神奈川県横浜市, 2016 年 11 月. (査読無)
[P20] 小川秀貴, 山口由紀子, 嶋田創, 高倉弘喜, 秋山満昭, 八木毅, "リクエスト間隔とレスポンスのボディサイズに基づくマルウェア感染由来の HTTP トラフィック検知," コンピュータセキュリティシンポジウム 2016, 2F1-3, pp. 408-415, 秋田県秋田市, 2016 年 10 月. (査読無)
[P21] 飛山駿, 山口由紀子, 嶋田創, 秋山満昭, 八木毅, "プロセスの挙動に着目した Deep Neural Network 多段利用によるマルウェア推定手法," コンピュータセキュリティシンポジウム 2016, 2B4-1, pp. 310-317, 秋田県秋田市, 2016 年 10 月. (査読無)
[P22] 多田竜之介, 小林良太郎, 嶋田創, "アノマリ検知複合のための機械学習ベースアノマリ検知手法の予備評価," 平成 28 年度電気・電子・情報関係学会東海支部連合大会, F3-7, 愛知県豊田市, 2016 年 9 月. (査読無)
[P23] Anri Suzuki, Ryotaro Kobayashi, and Hajime Shimada, "Instruction Rearrangement and Path Limitation for ALU Cascading," In Proceedings of the 2016 International Conference on Advanced Informatics: Concepts, Theory and Application (ICAICTA2016), DOI: 10.1109/ICAICTA.2016.7803081, Penang / Malaysia, August 2016. (査読有)
[P24] Kaoru Saito, Ryotaro Kobayashi, and Hajime Shimada, "Reduction of Cache Energy by Switching between L1 High Speed and Low Speed Cache under application of DVFS," In Proceedings of the 2016 International Conference on Advanced Informatics: Concepts, Theory and Application (ICAICTA2016), DOI: 10.1109/ICAICTA.2016.7803082, Penang / Malaysia, August 2016. (査読有)
[P25] Shun Tobiyama, Yukiko Yamaguchi, Hajime Shimada, Tomonori Ikuse, and Takeshi Yagi, "Malware Detection with Deep Neural Network Using Process Behavior," In Proceedings of the 6th IEEE International Workshop on Network Technologies for Security, Administration and Protection (NETSAP 2016), pp. 577-582, DOI: 10.1109/COMPSAC.2016.151, Atlanta / USA, June 2016. (査読有)
[P26] Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, and Hiroki Takakura, "An Automated ACL Generation System for Secure Internal Network," In Proceedings of the 6th IEEE International Workshop on Network Technologies for Security, Administration and Protection (NETSAP 2016), pp. 559-564, DOI: 10.1109/COMPSAC.2016.54, Atlanta / USA, June 2016. (査読有)

〔図書〕(計 0 件)

〔産業財産権〕
○出願状況(計 0 件)
○取得状況(計 0 件)

〔その他〕
ホームページ等
http://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/architecture.html
http://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html

６．研究組織

(1)研究分担者

研究分担者氏名：小林 良太郎

ローマ字氏名：KOBAYASHI Ryotaro

所属研究機関名：工学院大学(2017 年 3 月まで豊橋技術科学大学)

部局名：情報学部

職名：准教授

研究者番号（8 桁）：40324454

(2)研究協力者

なし