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　 ６ 月　 ６ 日現在

機関番号：５３９０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１８２５

研究課題名（和文）仮想計算機モニタの時系列メモリ証拠保全機構と深層学習によるインシデントの自動検出

研究課題名（英文）Hypervisor-based memory acquisition and restoration system for temporal-dimension forensic analysis and its application to deep-learning-based automatic incident detection

研究代表者

平野　学（Hirano, Manabu）

豊田工業高等専門学校・情報工学科・教授

研究者番号：５０３９０４６４

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）：本研究ではサイバー攻撃の監視・解析システムを国産の仮想計算機モニタと深層学習モデルを用いて開発した。本研究は以下の3つのテーマからなる：テーマ(A)では仮想計算機モニタBitVisorを用いて差分メモリダンプ取得機構を開発した。テーマ(B)ではテーマ(A)を用いて耐解析機能を持つランサムウェアBlueSkyを監視，メモリフォレンジックフレームワークVolatilityで解析した。テーマ(C)ではBitVisorでメモリアクセスパターンを収集し，深層学習でランサムウェアをFスコア0.98で検知できることを示した。

研究成果の学術的意義や社会的意義
今日のサイバーセキュリティが直面する課題は（１）サイバー犯罪の増大に警察など法執行機関が対処できなくなっていること，（２）ファイルレスマルウェア等の攻撃手法の高度化、暗号化ファイルシステムによってストレージフォレンジック技術が役に立たなくなってきていること，（３）犯罪者による証拠隠滅や改ざんへの対策が不可欠になっていること，の３点である。本研究ではこれらへの対策として，コンピュータの「監視システム」と大量の監視記録から証拠を高速に発見する「解析システム」を開発，評価した。本研究課題の成果はデジタルフォレンジック分野の主要ジャーナル Digital Investigation に採録された。

研究成果の概要（英文）：We developed a cyber-attack monitoring and analysis system using a lightweight hypervisor and a deep learning model. This study has three themes: in theme (A), we developed an incremental memory dump acquisition mechanism using a lightweight hypervisor, BitVisor. In theme (B), we used theme (A) to monitor BlueSky, a ransomware with anti-analysis capabilities, and we analyzed it using Volatility, a memory forensics framework. We published the results in the top international journal in digital forensics, Digital Investigation. In theme (C), we collected memory access patterns using BitVisor. The deep learning model trained using the memory access patterns could detect ransomware with an F-score of 0.98.

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　デジタルフォレンジック　仮想化技術　ランサムウェア検知　メモリフォレンジック　仮想計算機モニタ　ハイパーバイザ

様　式　Ｃ－１９，Ｆ－１９－１（共通）

１．研究開始当初の背景

今日のサイバーセキュリティが直面する課題は（１）サイバー犯罪の増加に警察などの法執行機関，官公庁，民間企業が対処できなくなってきていること，（２）ファイルレスマルウェア等の攻撃手法の多様化，暗号化ファイルシステムの活用等により従来のストレージフォレンジック技術が役に立たなくなってきていること，（３）犯罪者による証拠隠滅や改ざんへの対策がこれまで以上に必要とされていること，の３点である。本研究ではこれらの対策として，コンピュータシステムの挙動を記録する「監視システム」，それから得られる大量の監視記録から証拠を高速に発見する「解析システム」からなるサイバー攻撃への新しい対策機構を実装・評価する。

研究の学術的背景は以下の通りである。

（１） 仮想計算機モニタのセキュリティ研究への応用：本研究で扱う BitVisor はセキュリティに特化した仮想計算機モニタである。これまでソースコードが公開されていないオペレーティングシステム（OS）が官公庁ならびに民間企業で利用されてきた。仮想計算機モニタは OS よりも高い特権レベルで動作するため，このような内部構造が明らかでない OS に対して透過的にセキュリティ機能を強制する基盤となり得る。以上の理由から国産の仮想計算機モニタ BitVisor [1] が開発された。

（２） ディジタルフォレンジックの研究動向：デジタルフォレンジックはインシデントレスポンスや法的紛争・訴訟に際し，電磁的記録の証拠保全及び調査・分析を行い，改ざん・毀損等についての分析・情報収集等を行う科学的調査手法技術である（デジタルフォレンジック研究会の定義)。近年はフォレンジック機構への回避攻撃が問題になっている。本研究では仮想計算機モニタ BitVisor[1]を用いてメモリダンプを時系列で保全する機構を開発，評価した。この機構はたとえ OS が攻撃を受けたとしても機能し続ける。よって従来の OS で動作するフォレンジック機構に追加して多層防御を実現できる。

（３） 機械学習，深層学習のディジタルフォレンジック応用：ディジタルフォレンジックは特定領域の専門知識（例：ストレージフォレンジック，メモリフォレンジック等）が必要であり専門家が不足している。これらの特定領域専門家（Subject-matter experts）の知識を機械学習により補完することで，インシデントの検出，証拠の解析を自動化することが求められている。

[1] T. Shinagawa, H. Eiraku, K. Tanimoto, K. Omote, S. Hasegawa, T. Horie, M. Hirano, K. Kourai, Y. Oyama, E. Kawai, K. Kono, S. Chiba, Y. Shinjo and K. Kato. “Bitvisor: a thin hypervisor for enforcing I/O device security.” In Proc. of the 2009 ACM SIGPLAN/SIGOPS International conference on VEE, pp. 121-130, 2009.

２．研究の目的

本研究ではファイルレスマルウェア等のストレージに証拠を残さないタイプの攻撃に対抗するため，国産の仮想計算機モニタ BitVisor を用いて，OS を動作させながら時系列でメモリダンプを高速取得する「差分メモリダンプ取得機構」を開発する。その後，開発した機構の有用性を示すために耐解析機能を備えた BlueSky ランサムウェアのメモリダンプを取得してフォレンジック解析が可能かを検証する。以上に加えて，仮想計算機モニタ BitVisor を用いてメモリアクセスパターンを収集する機構を別に開発し，機械学習によってランサムウェアと良性プログラムを分類することが可能であるかを検証する。

３．研究の方法

本研究ではサイバー攻撃の監視・解析システムの開発と検証を，以下の 3 つのサブテーマによって実施した：テーマ(A)では国産の仮想計算機モニタ BitVisor を用いて「差分メモリダンプ取得機構」を開発した。テーマ(B)ではテーマ(A)で開発した監視システム用いて，耐解析機能を持つランサムウェア BlueSky を監視し，メモリフォレンジックフレームワーク Volatility で挙動を解析した。テーマ(C)では BitVisor でメモリアクセスパターンを収集し機械学習によってランサムウェアを検知できるかを検証した。

４．研究成果

テーマ(A)　差分メモリダンプ取得機構の開発

仮想計算機モニタ BitVisor を拡張して新たに「差分メモリダンプ取得機構」を開発，評価した。この成果はディジタルフォレンジック分野の主要ジャーナル Digital Investigation に採録された[2]。図１に開発した差分メモリダンプ取得機構の処理を示す。横軸が時間を示しており，初回でフルダンプを取得後に一定時間ごとに書き込みのあったメモリページだけを取得する。開発したシステムの詳細な評価，最新研究との比較，考察を論文[2]にて報告した。

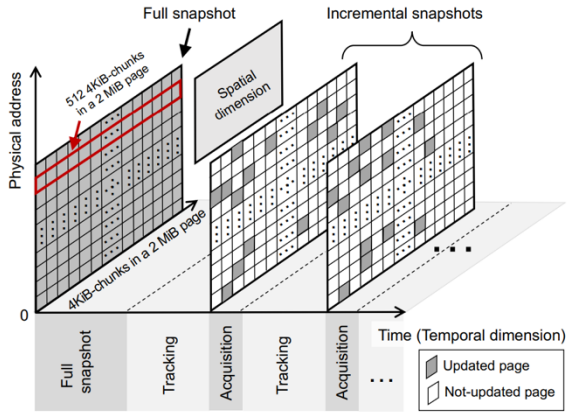

図１　差分型メモリダンプ取得機構[2]

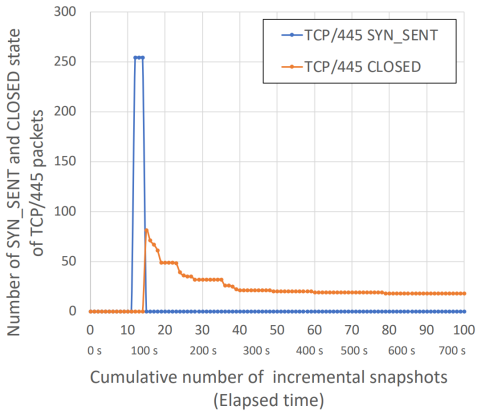

図２ BlueSky ランサムウェアの解析結果
（偵察パケット数の表示）[2]

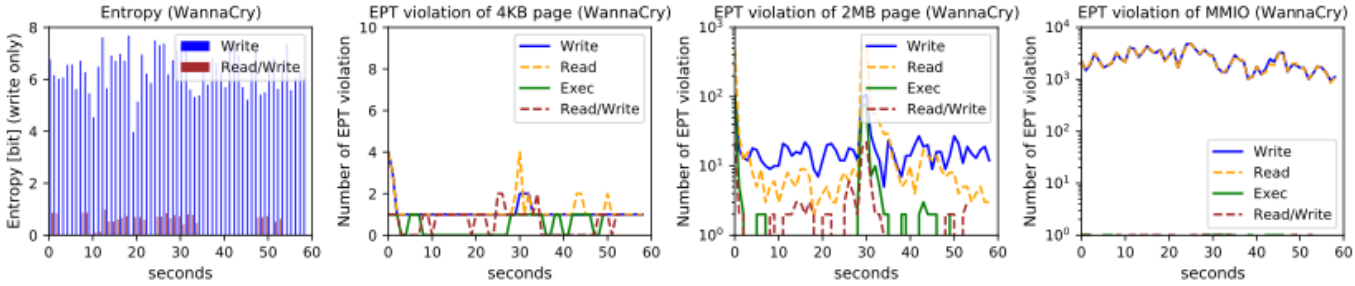

図３　WannaCry ランサムウェアのメモリアクセスパターン（60 秒間）[3]

テーマ(B) 耐解析機能を持つランサムウェアの解析
　テーマ(A)で開発した差分メモリダンプ取得機構を用いて，耐解析機能を備えた BlueSky ランサムウェアのメモリダンプを取得した。図２は差分メモリダンプから作成した時間経過ごとの TCP コネクション数の変化である。このグラフは特にランサムウェアが LAN 内で別マシンに感染する際に送信する TCP/445 パケットの TCP コネクション数の変化を示したものである。この結果から耐解析機能を有するランサムウェアであっても，本研究課題で開発した差分メモリダンプ取得機構で挙動を解析できることを示した。本解析に関する実験結果は論文[2]にて報告した。

テーマ(C) 仮想計算機モニタによるメモリアクセスパターン収集と機械学習による攻撃検知
　仮想計算機モニタ BitVisor のメモリ仮想化を利用してページ単位でのメモリアクセスパターンを収集する機構を開発した。図３は収集したランサムウェア WannaCry のメモリアクセスパターンのグラフである。ランサムウェアと良性プログラムを実行させ，メモリアクセスパターンを収集して機械学習モデルを訓練した結果，ランサムウェアを F スコア 0.98 で検知できたことを国際会議にて報告した[3]。

　研究期間にデジタルフォレンジック分野の主要ジャーナル Digital Investigation に仮想計算機モニタ BitVisor を用いたストレージ監視システムのデータセット公開論文が採録された[4]。本研究課題で収集したメモリアクセスパターンのデータセットならびにその解析論文も同じように公開する計画である。

[2] Hirano, M. and Kobayashi, R. “FIMAR: Fast incremental memory acquisition and restoration system for temporal-dimension forensic analysis.” Forensic Science International: Digital Investigation, 46, 301603, 2023, doi:10.1016/j.fsidi.2023.301603.
[3] Hirano, M. and Kobayashi, R. “Machine Learning-based Ransomware Detection Using Low-level Memory Access Patterns Obtained from Live-forensic Hypervisor.” In 2022 IEEE International Conference on Cyber Security and Resilience, pp. 323-330, 2022, doi:10.1109/CSR54599.2022.9850340.
[4] Hirano, M., Hodota, R., and Kobayashi, R. “RanSAP: An open dataset of ransomware storage access patterns for training machine learning models.” Forensic Science International: Digital Investigation, 40, 301314, 2022, doi:10.1016/j.fsidi.2021.301314.

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　2件）

１．著者名 Hirano Manabu、Kobayashi Ryotaro	４．巻 -
２．論文標題 Machine Learning-based Ransomware Detection Using Low-level Memory Access Patterns Obtained From Live-forensic Hypervisor	５．発行年 2022年
３．雑誌名 2022 IEEE International Conference on Cyber Security and Resilience (CSR)	６．最初と最後の頁 323 - 330
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/csr54599.2022.9850340	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 Hirano Manabu、Hodota Ryo、Kobayashi Ryotaro	４．巻 40
２．論文標題 RanSAP: An open dataset of ransomware storage access patterns for training machine learning models	５．発行年 2022年
３．雑誌名 Forensic Science International: Digital Investigation	６．最初と最後の頁 301314～301314
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.fsidi.2021.301314	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 Hirano Manabu、Kobayashi Ryotaro	４．巻 46
２．論文標題 FIMAR: Fast incremental memory acquisition and restoration system for temporal-dimension forensic analysis	５．発行年 2023年
３．雑誌名 Forensic Science International: Digital Investigation	６．最初と最後の頁 301603～301603
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.fsidi.2023.301603	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8件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 水野 広基，平野 学，小林 良太郎
２．発表標題 機械学習を用いたランサムウェア検知におけるメモリとストレージのアクセスパターンの特徴重要度の分析
３．学会等名 研究報告コンピュータセキュリティ（CSEC） 2022-CSEC-99(6)
４．発表年 2022年

１．発表者名
河根 範明，平野 学，小林 良太郎

２．発表標題
ストレージとメモリのアクセス速度の違いを考慮した深層学習によるランサムウェア検知システム

３．学会等名
研究報告コンピュータセキュリティ（CSEC） 2022-CSEC-99(7)

４．発表年
2022年

１．発表者名
牧原 京佑，平野 学，小林 良太郎

２．発表標題
準パススルー型ハイパーバイザーを用いた差分メモリダンプ機構の評価

３．学会等名
研究報告コンピュータセキュリティ（CSEC） 2022-CSEC-98(15)

４．発表年
2022年

１．発表者名
大森 貴通，平野 学，小林 良太郎

２．発表標題
準パススルー型ハイパーバイザを用いて取得したメモリデータの分析

３．学会等名
SCIS2022 暗号と情報セキュリティシンポジウム、2B3-1

４．発表年
2022年

１．発表者名
程田 凌羽，平野 学，小林 良太郎

２．発表標題
深層学習によるディスクアクセスパターンを用いたランサムウェア検知システム

３．学会等名
コンピュータセキュリティシンポジウム2021論文集、2021-10-19、1145-1150

４．発表年
2021年

１．発表者名
水野広基，牧原京佑，平野学，小林良太郎

２．発表標題
準パススルー型ハイパーバイザを用いたOSごとのメモリアクセスパターンの違いの調査

３．学会等名
令和3年度電気・電子・情報関係学会東海支部連合大会、H2-3

４．発表年
2021年

１．発表者名
程田 凌羽、平野 学、小林 良太郎

２．発表標題
ストレージアクセスパターンを用いた機械学習によるランサムウェア判別システムの精度向上に関する考察

３．学会等名
情報処理学会　研究報告コンピュータセキュリティ（CSEC）

４．発表年
2021年

１．発表者名
大森 貴通、水野 広基、牧原 京佑、平野 学、小林 良太郎

２．発表標題
準パススルー型ハイパーバイザによるメモリデータ収集機能の性能改善と評価

３．学会等名
情報処理学会　研究報告コンピュータセキュリティ（CSEC）

４．発表年
2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
RanSAP: An Open Dataset of Ransomware Storage Access Patterns
https://github.com/manabu-hirano/RanSAP

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