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　３ 年　 ６ 月 ２３ 日現在

機関番号：５３９０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2020
課題番号：１７Ｋ００１９８

研究課題名（和文）仮想計算機モニタを用いた法的証拠保全システムと機械学習による解析システムの高度化

研究課題名（英文）Hypervisor-based digital forensic evidence preservation system and its application to machine learning

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・准教授

研究者番号：５０３９０４６４

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：　本研究ではエンドポイントコンピュータ上のストレージ装置への入出力をハイパーバイザを用いて監視するシステムと，監視システムから取得した時系列データからセキュリティインシデントを自動的に検出する分析システムを開発した。本研究では分析システム上に新しい機械学習の機能を実装することで，先行研究のデータの断片を検索する分析システムを高度化した。開発したシステムをランサムウェア検体に適用し，収集したストレージアクセスパターンから96%-98%の精度（F値）でランサムウェアを検知できることを示した。本研究ではメモリフォレンジック機能の試作も完了した。以上により監視システムと解析システムの高度化を達成した。

研究成果の学術的意義や社会的意義
　本研究の学術的意義は以下の２点である。まず，（１）国産の軽量ハイパーバイザ BitVisor を用い，ゲストOSへの影響を最小限に抑えながら，観測対象プログラムのストレージ装置とメモリのアクセスパターンを収集する新しい機構を実装・評価した。さらに，（２）記録した時系列のストレージアクセスパターンを新たに機械学習に適用し，特に被害が急増しているランサムウェアの検知に応用できることを確かめた。ランサムウェア検体３種類と，ランサムウェアに類似したアクセスパターンをもつ良性プログラム３種類（暗号化，セキュア削除，圧縮）を学習させて 96%から98%の検知率（F値）を達成した。

研究成果の概要（英文）：In this project, we have developed the following two systems: a hypervisor-based surveillance system of storage devices on an endpoint computer, and an analysis system to find security incidents using the time-series data obtained from the surveillance system. The novel results of this project include: (1) we developed a novel machine learning feature on the analysis system. We used the machine-learning-based analysis system in detecting ransomware's storage access patterns. The system achieved a detection rate between 96% and 98% (F-measure). And (2) we developed a memory forensic feature on the surveillance system. In summary, we have refined our previous version of the hypervisor-based surveillance and analysis system using the machine-learning function and the memory forensic function.

研究分野：ディジタルフォレンジック，システムセキュリティ，ネットワークセキュリティ

キーワード：ディジタルフォレンジクス　ハイパーバイザ　ランサムウェア　機械学習　ストレージフォレンジクス　メモリフォレンジクス　仮想計算機モニタ　マルウェア

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

（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。BitVisor 開発の経緯は以下のようなものであった。日本の政府機関ではプロプラエタリな Microsoft 社の OS が幅広く利用されているが，このような内部構造が公開されていない OS を完全に信頼することは困難であるという問題があった。仮想計算機モニタは OS の更に下のレベルで動作するため，プロプラエタリな OS に対して透過的かつ強制的にセキュリティ機能を適用する基盤となる。このような理由で，仮想計算機モニタ BitVisor は科学技術振興調整費（2006 年度～2008 年度）の支援で開発され，現在まで BitVisor を活用した研究が活発に行われており，オープンソースでの開発が継続されている。

（２）デ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）。世界的な研究コミュニティとしては 2001 年から Digital Forensic Research Workshop (DFRWS) が開催され，本申請のテーマであるセクタ単位の高速なファイル検出手法（Garfinkel et al., DFRWS2015），メモリフォレンジック（Case et al., DFRWS2016），アンチフォレンジック(Conlan et al., DFRWS2016) 等の研究が行われている。本申請は解析システムに Garfinkel らの手法を採用しているほか，仮想計算機モニタ BitVisor に監視機能を実装してアンチフォレンジック攻撃に対抗している。本申請は新たにメモリフォレンジック機能を実装し，ストレージに証拠を残さないタイプの攻撃にも対応する。

（３）機械学習のデジタルフォレンジックへの応用

機械学習は 1950 年代に Samuel らによって創始された分野であり，近年は Hinton らが逆伝播法を多層ニューラルネットワークの学習に用いる Deep neural network を提案したことで識別精度が向上した。教師あり機械学習の主な用途はパターン認識，異常検出，将来予測の３つである。提案システムでは監視システムから得た大量の時系列のセクタデータを解析する必要がある。先行研究では監視データに含まれる個々のセクタ単位のデータを高速に検索する機構を既に実装しているが，本研究では新たに機械学習を用いてセキュリティインシデントを自動的に検出するデジタルフォレンジックの新しい解析システムを提案する。

２．研究の目的

セキュリティインシデントが増加することで，ディジタルフォレンジックの解析対象となるデータ量が増大し，サイバー犯罪に対処していけなくなってきている。さらに証拠隠滅や改ざんへの対策が不可欠になってきている。本研究では国産の軽量ハイパーバイザ BitVisor を監視システムとして採用することで，セキュリティインシデントの原因を記録し，解析サーバに自動的に転送する。解析システムでは分散並列処理による高速なデータの断片の検索（先行研究にて開発済み）に加えて，本研究で新たに機械学習を用いてセキュリティインシデントを自動的に検出する機構を設計，実装，評価する。BitVisor による監視システムを現実世界の監視カメラに例えると，本研究の解析システムの役割は大量かつ長時間の映像から自動的に犯人を見つけ出す機械学習モデル（人工知能）に相当する。

３．研究の方法

先行研究（科研費 2014-2016）で既にハイパーバイザ BitVisor を用いた監視システムを開発している。同様に先行研究（科研費 2014-2016）にて監視システムで得られたストレージ装置の書き込みデータを解析するシステムも開発している。解析システムは Hadoop と Apache Spark による分散並列処理クラスタで動作するように実装されており，過去に書き込まれたデータをセクタ単位のハッシュ値を用いて高速に検索するものである。たとえば悪性プログラムやセキュリティインシデントに関連するファイルを解析システムに与えると，そのファイルをセクタ単位に分割して過去の大量の書き込みデータから検索し，その時刻でのストレージ装置のイメージを復元することができる[6]。

本研究ではこの解析システムが処理する書き込まれたセクタのエントロピー，読み書きされ

たデータ量，読み書きされた番地（Logical Block Address）の分散を特徴量として学習させ，ランサムウェアを自動的に検出する機構を設計，実装，評価した。さらに，ストレージ装置のアクセスパターンだけではなく，近年増加しているファイルレスマルウェア（ストレージ装置に痕跡を残さず，ストレージフォレンジックでは検出できないマルウェア）に対応するため，監視システム上で新たにメモリフォレンジック機能を試作した。

４．研究成果

本研究では先行研究（科研費 2014-2016）の解析システムに機械学習を適用し，代表的なセキュリティインシデントとしてランサムウェアのストレージアクセスパターンを検出するシステムを設計，実装，評価した[1][2][3]。この研究ではランサムウェアを隔離環境において動作させ，そのストレージ装置へのアクセスパターンを収集した。ランサムウェアは被害者のコンピュータにあるファイルを暗号化して身代金（ランサム）を要求する悪性ソフトウェアであるため，ストレージ装置のアクセスパターンに特徴が現れるという仮説を立てた。検証にあたってはランサムウェアと類似したアクセスパターンを持つ良性プログラム（圧縮プログラム Zip，セキュア削除プログラム SDelete，暗号化プログラム AESCrypt）をデータセットに加えて検知率を評価した。ランサムウェアは WannaCry，TeslaCrypt，Cerber のアクセスパターンを収集して評価した。図１から図６に特徴量をグラフにしたものを示す。これらの特徴量を Random Forest，Support Vector Machine（SVM），k-Nearest Neighbors（kNN）の３つの機械学習アルゴリズムで学習させた結果，96% の精度（F 値）[2]でランサムウェアと良性プログラムを分類することができた。研究成果[1]では WannaCry，TeslaCrypt，Zip の３分類問題で 98%の F 値を得た。

図 1　WannaCry のストレージ装置へのアクセスパターン

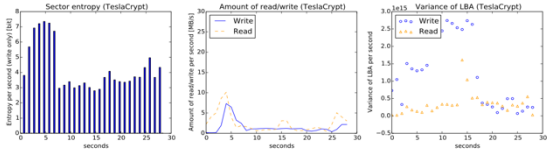

図 2　TeslaCrypt のストレージ装置へのアクセスパターン

図 3　Cerber のストレージ装置へのアクセスパターン

図 4　Zip のストレージ装置へのアクセスパターン

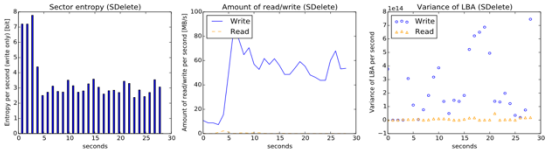

図 5　SDelete のストレージ装置へのアクセスパターン

図 6　AESCrypt のストレージ装置へのアクセスパターン

[1] Hirano, M., & Kobayashi, R. (2019, October). Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained From Live-forensic Hypervisor. In Proceedings of Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp.1-6, IEEE, 2019.
[2] 程田 凌羽，今泉 大慈郎，平野 学，小林 良太郎，ストレージアクセスパターンに着目した機械学習及び深層学習によるランサムウェアの検知手法の検討，情報処理学会 研究報告コンピュータセキュリティ（CSEC），2020-CSEC-88(19)，pp.1-8，2020 年 3 月.
[3] 池田征士朗，高直我，平野学，小林良太郎，ストレージアクセス履歴の時系列解析システムの実装とランサムウェア解析への応用，情報処理学会 研究報告コンピュータセキュリティ（CSEC），2018-CSEC-83（10），pp.1-7，2018 年 12 月 6 日.

特に研究成果[2]ではアクセスパターンの特徴ベクトルを画像化して，畳み込みニューラルネットワークで深層学習させる実験も実施した。図７から図１２に横軸が経過時間，縦軸がストレージ装置の番地（read が左，write が右）のヒートマップを示す。赤色はアクセス数が多い部分を示している。同様に，図１３から図１８には Gramian Difference Angular Field (GADF)アルゴリズムによって特徴ベクトルを画像化したものを示す。これらの画像を ResNet50 モデルで転移学習させ，前者のヒートマップでは 71.8%，後者の GADF 画像では 88.9% の正解率を得た。

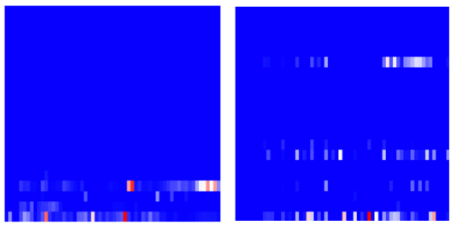

図 7　WannaCry のヒートマップ（左：Read，右：Write）

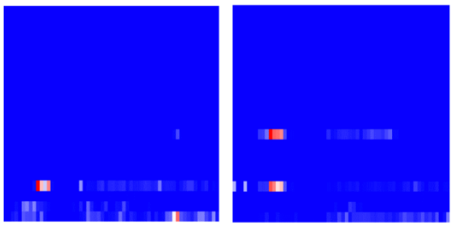

図 8　TeslaCrypt のヒートマップ（左：Read，右：Write）

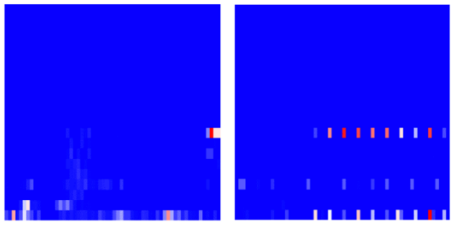

図 9　Cerber のヒートマップ（左：Read，右：Write）

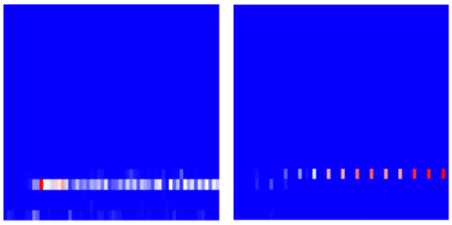

図 10　Zip のヒートマップ（左：Read，右：Write）

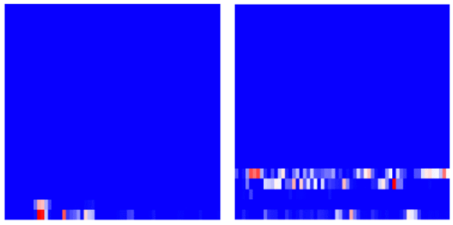

図 11　SDelete のヒートマップ（左：Read，右：Write）

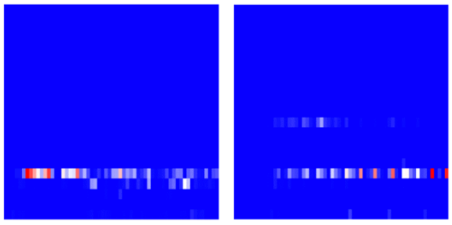

図 12　AESCrypt のヒートマップ（左：Read，右：Write）

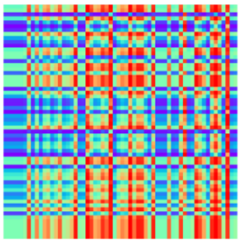

図 13　WannaCry の GADF 画像

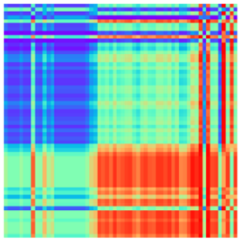

図 14　TeslaCrypt の GADF 画像

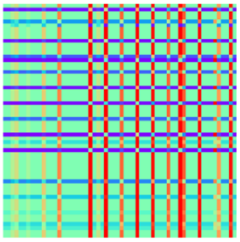

図 15　Cerber の GADF 画像

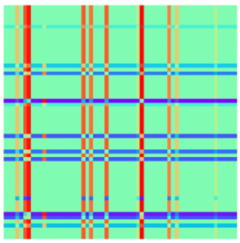

図 16　Zip の GADF 画像

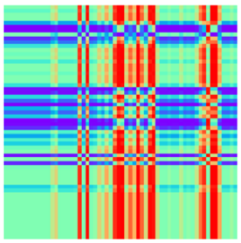

図 17　SDelete の GADF 画像

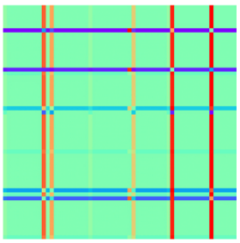

図 18　AESCrypt の GADF 画像

また，先行研究（科研費 2014-2016）の監視システムへメモリフォレンジック機能を追加する試作をおこなった[4]。図１９に試作したメモリフォレンジック機能の構成を示す。今回はゲスト OS に補助プログラムを動作させることで，監視対象プロセスの仮想アドレスを物理アドレスに変換し，その物理アドレスを BitVisor が収集してサーバへ UDP 転送する機構を試作，評価した。

[4] 大森 貴通，稲垣 怜，平野 学，小林 良太郎，準パススルー型ハイパーバイザーを用いた時系列メモリデータ取得機能の試作と評価， 情報処理学会 研究報告コンピュータセキュリティ（CSEC），2020-CSEC-88(14)，pp. 1-6，2020 年 3 月.

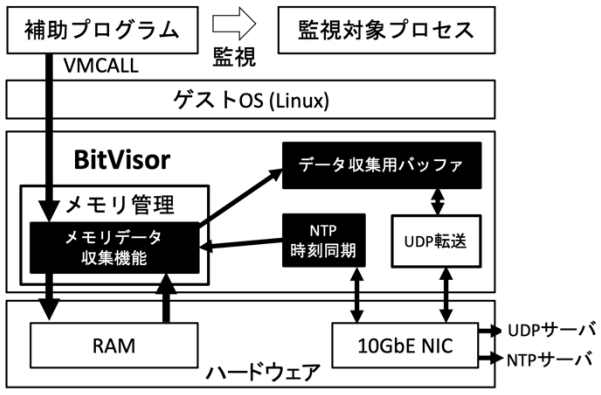

図 19 メモリデータ取得機能の構成

図２０に試作したメモリフォレンジック機能のフローチャートを，図２１に監視システムである BitVisor が転送するデータ（仮想アドレス，サイズ，時刻，フラグ，データ本体）を示す。

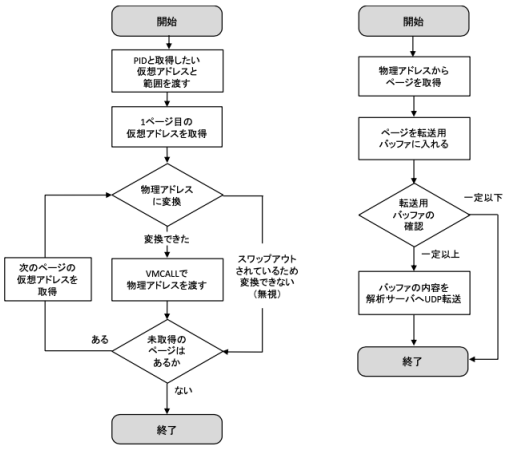

図 20　処理の流れ（左：ユーザランドの補助プログラム，右：ハイパーバイザーのメモリデータ収集機能）

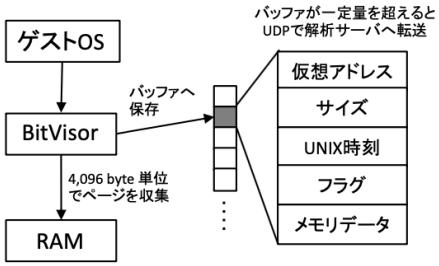

図 21　ハイパーバイザの転送用バッファ

試作したメモリフォレンジック機能のスループットを実験で確かめた結果を図２２に示す。この実験では malloc で確保するメモリ領域のサイズを変化させ，その領域にあるページを収集したときのスループットを計測した。最大スループットは 500 MB を収集したときの 190.7 MB/s であった。また，同様にメモリ確保するサイズを変更したときの BitVisor 側での処理時間（VMCALL 実行時間）を計測した（図２３）。この実験により VMCALL １回につき平均 19.4 ns かかっていることを確認した。

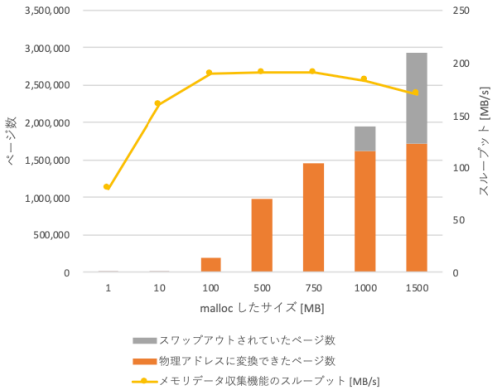

図 22　メモリデータ収集機能のスループット

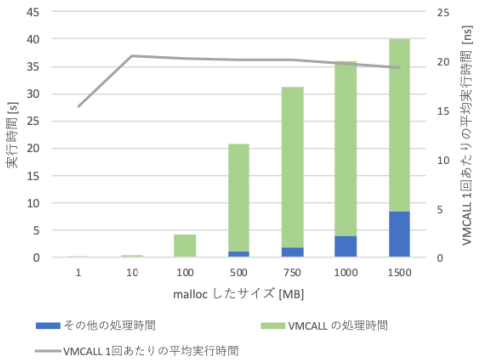

図 23　VMCALL 実行時間

以上のメモリフォレンジック機能の試作と評価を通して，先行研究（科研費 2014-2016）の監視システムをベースとしたメモリフォレンジック機能を試作できた。これによって，ストレージ装置に痕跡を残さない高度なサイバー攻撃の検知に提案システムを利用できる目処が立った。

上記以外の研究成果として，監視システムの実装と評価実験の結果を論文にまとめて発表した[5]。また，Infrastructure as a Service (IaaS)クラウドコンピューティング基盤で解析システムを用い，高速にインシデントの証拠ファイルをセクタハッシュで高速に検索し，過去のストレージ装置の状態を復元するフォレンジック機構を実装，評価した結果を論文で発表した[6]。

[5] M. Hirano, N. Tsuzuki, S. Ikeda, N. Taka, K. Fujiwara, and R. Kobayashi. "Waybackvisor: Hypervisor-based scalable live forensic architecture for timeline analysis." In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, pp. 219-230. Springer, Cham, 2017.
[6] M. Hirano, N. Tsuzuki, S. Ikeda, and R. Kobayashi. "LogDrive: a proactive data collection and analysis framework for time-traveling forensic investigation in IaaS cloud environments." Journal of Cloud Computing, 7, no. 1 (2018): 1-25, Springer.

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　1件）

１．著者名 Hirano, M., Tsuzuki, N., Ikeda, S., and Kobayashi, R	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, Springer	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） 10.1186/s13677-018-0119-2	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Hirano, M., Tsuzuki, T., Ikeda, S., Taka, N., Fujiwara, K., and Kobayashi, R.	４．巻 －
２．論文標題 WaybackVisor: Hypervisor-Based Scalable Live Forensic Architecture for Timeline Analysis.	５．発行年 2017年
３．雑誌名 In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage	６．最初と最後の頁 219-230
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-72395-2_21	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、Kobayashi Ryotaro	４．巻 －
２．論文標題 Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained From Live-forensic Hypervisor	５．発行年 2019年
３．雑誌名 In proceedings of Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE	６．最初と最後の頁 1, 6
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/IOTSMS48152.2019.8939214	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 －

〔学会発表〕　計9件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 大森貴通，稲垣怜，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メモリフォレンジックの提案
３．学会等名 電気・電子・情報関係学会東海支部連合大会
４．発表年 2019年

１．発表者名
程田凌羽，今泉大慈郎，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と機械学習を用いたランサムウェアの検知システム

３．学会等名
電気・電子・情報関係学会 東海支部連合大会 - IEEE学生奨励賞 (Nagoya Section Student Paper Award)

４．発表年
2019年

１．発表者名
程田凌羽，今泉大慈郎，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に注目した機械学習及び深層学習によるランサムウェアの検知手法の検討

３．学会等名
第88回 情報処理学会コンピュータセキュリティ (CSEC) 研究会

４．発表年
2020年

１．発表者名
大森貴通，稲垣怜，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時系列メモリデータ取得機構の試作と評価

３．学会等名
第88回 情報処理学会コンピュータセキュリティ (CSEC) 研究会

４．発表年
2020年

１．発表者名
池田征士朗 ，高直我 ，平野学 ，小林良太郎

２．発表標題
ストレージアクセス履歴の時系列解析システムの実装とランサムウェア解析への応用

３．学会等名
情報処理学会コンピュータセキュリティ研究会

４．発表年
2018年

１．発表者名
高直我 ， 池田征士朗 ， 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ストレージアクセスパターンの収集システムの提案

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム

４．発表年
2018年

１．発表者名
高直我，都築卓馬，藤原賢二，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によるストレージ装置の読み書き監視システム

３．学会等名
電気・電子・情報関係学会東海支部連合大会 C4-1

４．発表年
2017年

１．発表者名
池田征士郎，都築夏樹，藤原賢二，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ランサムウェアのディスクアクセスパターンの解析に向けた 取り組み

３．学会等名
電気・電子・情報関係学会東海支部連合大会 C4-2

４．発表年
2017年

１．発表者名
都築卓馬，岡野兼也，高直我，平野学

２．発表標題
準パススルー型ハイパーバイザーを用いたブロックデバイス監視システムの性能評価

３．学会等名
情報処理学会第79回全国大会 1W-01

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

国際ジャーナル（Journal of Cloud Computing, Springer）で発表したシステム LogDrive のソースコード公開ページ https://github.com/manabu-hirano/logdrive

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