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

平成　２９　年　　６　月　２６　日現在

機関番号：　５３９０１
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１６８

研究課題名（和文）仮想計算機を用いた法的証拠の保全システムと分散並列処理による解析システムの融合

研究課題名（英文）Development of a Digital Forensic System for Preserving Digital Evidence by Using Virtual Machine Monitors and Distributed Parallel Processing Frameworks

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）　　3,100,000円

研究成果の概要（和文）：機密情報を扱ったり社会基盤を制御するコンピュータ・システムはサイバー攻撃に対して脆弱である可能性がある。本研究の目的はこのような重要度の高いコンピュータ・システムを監視するシステムを開発することであった。このシステムは、第一にストレージ装置へのすべての入出力を監視してデータを保全し、第二に大量の監視データから分散並列処理で高速に証拠と発生日時を特定し、第三に事件発生時のディスク状態を復元し法的証拠を提示するためのものである。本研究の主要な成果は、クラウド向けとクライアント向けの２種類の監視システムとフォレンジッククラスタ向けの解析システムを開発したことである。

研究成果の概要（英文）：Computer systems that process confidential information or control critical infrastructures are potentially vulnerable to cyber attacks. The project's goal is to develop a digital forensic system that achieves the following functions: (1) preserving all input and output on storage devices, (2) analyzing the preserved data by using distributed parallel processing, and (3) restoring the monitored storage device at an arbitrary point in time for providing law-enforcement agencies with evidence. The key outcomes are the follows: (1) surveillance and analysis system for Infrastructure-as-a-Service cloud environments by using Xen hypervisor and a Hadoop cluster and (2) surveillance and analysis system by using BitVisor and a Hadoop cluster. These systems achieves high-throughput on preserving input and output on storage devices. Furthermore, the system also accomplished high-throughput for finding known-good and known-bad files by using distributed sector-based hash algorithms.

研究分野：　情報セキュリティ

キーワード：　ディジタル・フォレンジック　証拠保全　インシデント・レスポンス　仮想計算機モニタ　分散並列処理　サイバー攻撃　監視

１．研究開始当初の背景

（１）ディジタル・フォレンジック（デジタル鑑識）とサイバー攻撃

近年はコンピュータ・システムに対するサイバー攻撃や悪用による事件事故が増加しており、コンピュータ・システムの操作記録（ログ）を保全することの重要度が増している。事件事故（インシデント）発生時には、速やかにディスクイメージや各種ログ、メモリダンプ等を分析し、証拠資料を作成し、場合によっては法廷へ提出する。しかしながら、攻撃者に意図的に消去されてしまったデータや上書きされてしまったデータは、証拠の復元が困難となる。過去に問題になったように、法執行機関によって証拠データのファイルシステム上のタイムスタンプが改ざんされ、冤罪を発生させる可能性も考えられる。多くのサイバー攻撃では攻撃者によってデジタルデータの証拠を消されたり、攻撃者の都合のよいように改ざんされてしまう。よって、これらの攻撃への対策が不可欠である。

（２）仮想計算機モニタのセキュリティへの応用

本研究で扱う仮想計算機モニタ BitVisor は Intel-VT を活用したクライアント側のセキュリティに特化した仮想計算機モニタである。現在、プロプラエタリな内部構造が公開されていないマイクロソフト社の OS が幅広く利用されているが、これらの OS に対してセキュリティ機能を強制させようとした場合に、OS を完全に信頼することが困難である問題があった。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様々なセキュリティ機能を強制させる基盤となり得る。本研究では Windows で動作するクライアントコンピュータ向けの監視には BitVisor を利用する。また、クラウド向けの監視システムには Xen ハイパーバイザを利用する。

２．研究の目的

本研究の目的は、以下に述べるサイバー攻撃への耐性を持つセキュリティ・システムを設計、開発、評価することであった。

まず、これまでの一般的なディジタル・フォレンジックの手法では事件発生後に証拠となるコンピュータ・システムや、それらに接続されていた通信機器を押収し、分析するのが一般的であった。しかしながら、社会基盤を制御するコンピュータや、企業で機密情報を扱うコンピュータについては、事前に監視システムを作動させておき、事件発生後に証拠を探すほうが効率的であり、経済的にも合理的である。たとえば、従来手法ではサイバー攻撃によって情報漏えいや制御システムへの不正操作があった場合でも、攻撃者によって証拠が削除されてしまえば、法廷などへ有効な証拠を提出できなかった。しかしながら、本研究で提案するような時系列ですべての入出力を監視し記録していくシステムを用いると、攻撃者の証拠隠滅の行動まで記録することができるようになる。このような証拠隠滅の手法はアンチ・フォレンジック攻撃と呼ばれている。本研究ではアンチ・フォレンジック攻撃に対抗するために、仮想計算機モニタを用いた監視システムを事前に動作させておき、すべての読み書きの記録を保存していく方法で解決を試みた。本研究の第一の目的はクラウド向けとクライアント向けの種類の監視システムを開発することであった。

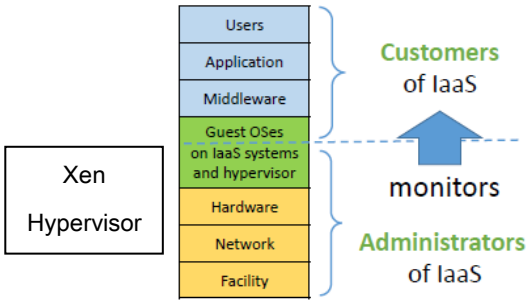

図１　クラウド監視システムの概念図

本研究の第二の目的は、ディジタル・フォレンジックで扱うデータ量が増加している問題の解決である。例えば、攻撃者は大量の偽の操作の中に本当の攻撃を紛れ込ませることで、ディジタル・フォレンジックに要するコストを増大させることができる。これは、a needle in a haystack、つまり干し草の山の中から針 1 本捜すような労力を要することを狙った攻撃である。さらに、消費者向けの HDD や SSD のディスク容量が増加して安価になっていることから、従来型のディジタル機器の犯罪捜査にも時間を要するようになってきている問題が生じている。その結果、データ量の増大に起因して、犯罪捜査の専門家が、ディジタル機器から証拠データを探しだす時間やコストが増加している。本研究では、以上で述べた解析対象データの増大問題に対して、分散並列処理を提供する小規模なクラスタ（法執行機関でも利用できる程度の計算機）を用いて解決を試みた。犯罪捜査で解析対象となるような機密性の高いデータはパブリック・クラウドの処理には適さないため、本研究では実際に小規模クラスタで解析システムを実装することにした。

３．研究の方法

我々は前の科研費の研究（**課題番号**：２３７００９５）において、すべてのストレージ装置への書き込み履歴を追記で保管していくデータ形式を定義し、それを読み書きするデバイスドライバを開発した。本研究ではその先行研究を拡張するかたちで、コンピュータ・システムを監視する機構を開発した。

本研究では、図１に示すようにクラウドコ

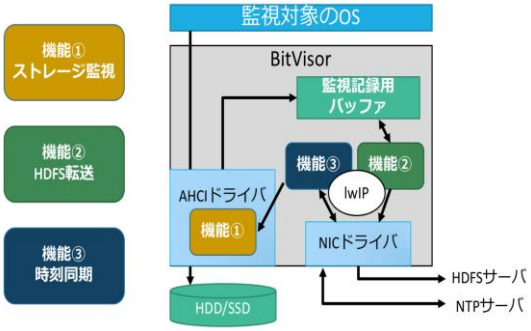

図２　クライアント向けの監視システム

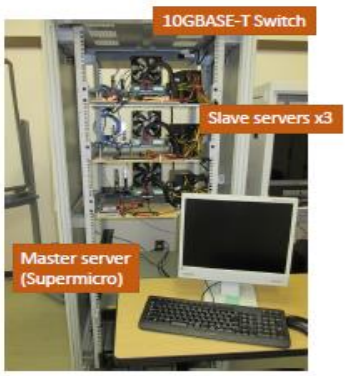

図３　解析用フォレンジック・クラスタ

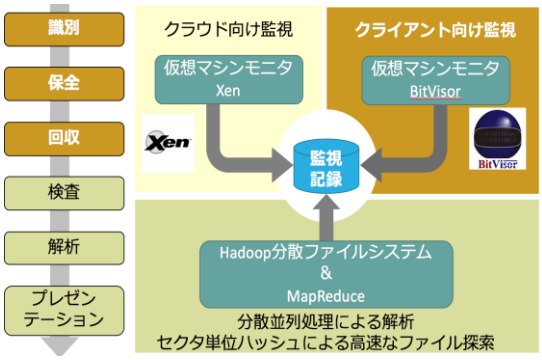

図４　本研究における２種類の
監視システムと解析システムの構成図

ンピューティングを提供するサーバ向けの監視システムを Xen ハイパーバイザを用いて開発し、オフィスに設置されているクライアントコンピュータで動作する監視システムを国産ハイパーバイザである BitVisor を拡張するかたちで開発した（図２）。

上述の２種類の監視システムからは大量の監視データが生成される。そこで、我々はそれらの監視データを同じローカルエリアネットワークに設置されたフォレンジック・クラスタ（図３）の分散ファイルシステムへ転送する機構を開発した。本研究プロジェクト全体の各要素研究の構成を図４に示す。

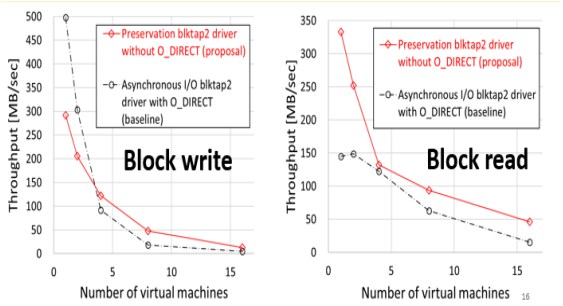

図５　クラウド向け監視システムの
性能評価実験の結果

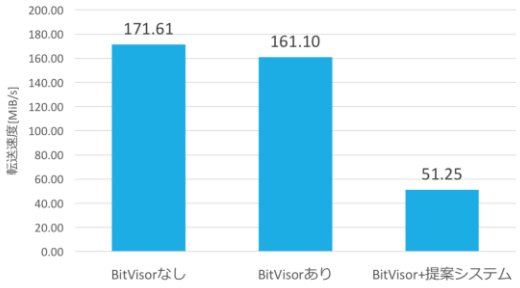

図６　クライアント向け監視システムの
性能評価実験の結果

４．研究成果

本研究の主要な成果を紹介する。

（１）監視システム：　クラウド向けは Xen を用いたシステムを開発した。クライアント向けは BitVisor を用いたシステムを開発した。両者とも性能評価をおこない、論文にて発表した。図５にクラウド向けの監視システムの性能評価の結果を示す。クラウド向けの監視システムは Log-structure と呼ばれる追記式のデータ構造であったため、４台以上の仮想マシンを同時に実行させたときに、通常の監視無しよりも逆に書き込み性能が向上する結果となった。逆に、Log-structure のデータ構造では読み込みの性能が低下する傾向にあるが、本研究で開発したシステムでは監視無しの時と比べて、大幅な読み込み性能の低下はなかった。クライアント向けの監視システムの書き込み性能の実験結果を図６に示す。監視有りの場合で 51.25 MB/s の性能であった。クライアント監視の場合には書き込まれたデータをリアルタイムで図３のクラスタへ転送する（クラウド向けはバッチ処理で定期的にクラスタへ転送している）。この際に、クライアントの 1GbE のネットワークカード経由で、我々が実装した WebHDFS プロトコルでデータ転送している。1GbE ネットワークカードの理論上の転送上限が 128 MB/s であるので性能改善の余地がある。一般的な消費者向け HDD の転送速度と比べても極端に遅いわけではないため実用に耐えるシステムを実現できたといえるが、現在も継続して性能向上のため改良を実施している。

（2）解析システム： 上記の２種類のシステムから得られた監視システムを４台から構成される小規模なクラスタで並列処理させることで、高速に目的のファイルを検索したり、不要なファイルを除外できることを示した。ファイルの検索には、ファイルをセクタ単位に分割して、それぞれのハッシュ値を計算する手法（Garfinkel, et al., 2010）を採用して評価実験をおこなった。解析結果は[雑誌論文]の文献②に示した。さらに、本研究では類似ハッシュと呼ばれる完全一致ではないデータを発見するためのアルゴリズムを解析システムに採用して評価を行った。類似ハッシュには sdhash アルゴリズム（Roussev, 2010）を用いて評価を行った。

＜引用文献＞

① Garfinkel, Simson, et al. ″Using purpose-built functions and block hashes to enable small block and sub-file forensics.″ digital investigation 7 (2010): S13-S23.
② Roussev, Vassil. ″Data fingerprinting with similarity digests.″ IFIP International Conference on Digital Forensics. Springer Berlin Heidelberg, 2010.

５．主な発表論文等

〔雑誌論文〕（計２件）

① Manabu Hirano and Hiromu Ogawa, A Log-structured Block Preservation and Restoration System for Proactive Forensic Data Collection in the Cloud, In Proceedings of the 11th International Conference of Availability, Reliability and Security (ARES 2016), pp. 355-364, Salzburg, Austria, September 2016, DOI: 10.1109/ARES.2016.8, 査読有
② Manabu Hirano, Hayate Takase, and Koki Yoshida. Evaluation of a Sector-Hash Based Rapid File Detection Method for Monitoring Infrastructure-as-a-Service Cloud Platforms, In Proceedings of the 10th International Conference of Availability, Reliability and Security (ARES2015), pp. 584-591, Toulouse, France, August 2015, DOI: 10.1109/ARES.2015.15, 査読有

〔学会発表〕（計 10 件）

① 都築卓馬、岡野兼也、高直我、平野学. 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. 情報処理学会第 79 回全国大会、名古屋大学（愛知県）、 pp. 1W-01、March 2017、 査読無
② 吉田光輝、 池田征士朗、 原田滉史、 平野学. ブロック単位でのディスクへの書き込み履歴から異常検出する手法の評価. 情報処理学会第 79 回全国大会、 名古屋大学(愛知県)、 pp.1W-02、March 2017、 査読無
③ 都築夏樹、 平野学. 4KiB ブロックごとの類似ハッシュの検出性能の評価. 情報処理学会第 79 回全国大会、 名古屋大学（愛知県)、 pp. 1W-03、 March 2017、 査読無
④ 都築卓馬、平野学. セキュリティインシデントの証拠発見を支援するブロックストレージの書き込み監視システム. 電気・電子・情報関係学会東海支部連合大会、 豊田高専（愛知県)、 pp. F3-3、 September 2016、 査読無
⑤ 吉田光輝、平野学. セキュリティインシデント対応のための時系列データの可視化と証拠発見支援. 電気・電子・情報関係学会東海支部連合大会、 豊田高専(愛知県)、 pp. F3-4、 September 2016、 査読無
⑥ 都築夏樹、平野学. セキュリティインシデント対応のための類似度の高いファイルの検出手法. 電気・電子・情報関係学会東海支部連合大会、 pp. F3-5、 September 2016、 査読無し、 IEEE 名古屋支部学生奨励賞
⑦ 都築卓馬、平野学. 準パススルー型ハイパーバイザを利用したブロックストレージの書き込み監視システム. 情報処理学会第 78 回全国大会、 慶応義塾大学矢上キャンパス(横浜市)、 pp. 2W-06、March 2016、 査読無、 学生奨励賞受賞
⑧ 都築夏樹、 平野学. Similarity digest システムの 4kib ブロックデータへの適用と評価. 情報処理学会第 78 回全国大会、 慶応義塾大学矢上キャンパス（横浜市)、 pp. 2W-07、 March 2016、 査読無
⑨ 吉田光輝、 高瀬誉、 平野学. 仮想計算機モニタを用いた外部記憶装置の監視分析システム～ブロックハッシュを用いた分析機能の試作と評価. 情報処理学会第７７回全国大会、京都大学(京都府)、pp. 5X-05、 March 2015、 査読無
⑩ 平野学、 吉田光輝、 高瀬誉. セクタハッシュと並列分散処理を用いた大量の書き込み履歴データからの目的ファイルの高速な検出. 研究報告コンピュータセキュリティ（CSEC)、 法政大学小金井キャンパス(東京都)、 第 2015-CSEC-68 巻、 pp. 1-8、 March 2015、 査読無

〔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

６．研究組織
(1)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

(2)研究分担者
なし

(3)連携研究者
なし

(4)研究協力者
David Chadwick (CHADWICK, David)