様式Ｆ－１９

科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

平成２５年６月１３日現在

機関番号：５３９０１
研究種目：若手研究（Ｂ）
研究期間： 2011 ～ 2012
課題番号：２３７０００９５
研究課題名（和文） 仮想計算機モニタを用いた電子データの操作履歴と法的証拠の改ざん検出を行うシステム
研究課題名（英文） Development of a Novel Digital Forensics System based on Virtual Machine Monitors
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

研究成果の概要（和文）： 本課題では仮想計算機モニタを用いて電子データの操作履歴を記録し，法的証拠となるデータを保護するシステムを実現するための研究開発を行った．本課題の２年間の開発成果は，(1) 仮装計算機モニタ Xen で動作する，操作履歴を自動保存し紛争調査時に任意時刻への復元を行うシステムと，(2) 仮装計算機モニタ BitVisor へのロールベースアクセス制御システムの組み込みである．開発成果(1)はソースコードを公開した．

研究成果の概要（英文）： The purpose of this project is to develop a novel digital forensic system based on hypervisor. The system has data preservation and restoration mechanism for protecting digital evidence. I developed the following essential programs to construct the digital forensics system: (1) Data preservation and restoration system for Xen hypervisor and (2) Role-based access control modules for BitVisor, security-purpose hypervisor. I released the source code of the data preservation and restoration system for Xen hypervisor on my web site.

交付決定額

（金額単位：円）

	直接経費	間接経費	合 計
交付決定額	1,700,000	510,000	2,210,000

研究分野：情報セキュリティ
科研費の分科・細目：１００３・Ｂ
キーワード：仮想計算機モニタ，ディジタルフォレンシックス，証拠保全

１．研究開始当初の背景

仮想計算機モニタ（Virtual Machine Monitor または Hypervisor と呼ばれる）は 1960 年代に IBM 社のメインフレーム System/360 向けの CP/CMS 等として発明された．その後しばらくはメインフレームコンピュータの計算機資源を有効活用するために利用されていたが，1998 年にスタンフォード大学の Rosenblum 教授が仮想化技術を PC に持ち込むことを提案し，後に VMware 社を設立した．2005 年にインテル社が仮想計算機モニタをハードウェアでサポートする CPU 命令（Intel Virtualization Technology, Intel-VT）をサポートしてから，VMware，Xen，Microsoft 社 Hyper-V などの多くの仮想計算機モニタが開発され，現在に至っている．

本課題では，情報を完全な状態で確実に保全し，犯罪捜査時に必要な情報を取り出し，証拠を分析しやすい環境を実現するために，補助記憶装置への書き込み履歴を保存し，任意の時刻の状態を復元するシステムを設計，実装する．本提案では，仮想計算機モニタによって補助記憶装置へ書き込もうとした情報をすべて保全する．OS 上で悪意のあるソフトウェアがファイルを削除・改竄した場合にも検出でき，攻撃を受ける前の情報を取り

出すことも可能なため，コンピュータ上で扱った情報を確実に保全できる．犯罪者やマルウェアの中には証拠となるファイルやアクセスログを改竄して証拠隠滅を図るものもあるが，そのような場合にも補助記憶装置への書き込み内容を仮想計算機モニタのレベルで時系列に保全することで隠滅行為がいつ起きたかを特定できる可能性が高くなる．提案システムで利用する仮想計算機モニタは，ハードウェアを疑似的に再現する環境を作り出すソフトウェアである．仮想計算機モニタは，ゲスト OS とは分離されることを目指して実装されているため，原則として OS 上での動作に影響を受けない．そのため，もし仮想計算機モニタの制御をゲスト OS の利用者から隔離することができれば，悪意のある利用者がシステムを停止させて履歴の保存を回避することはできなくなるはずである．

提案システムが想定するのは，企業や官公庁のような組織が管理するコンピュータシステムである．特にコンピュータの操作履歴やアクセス日時が記録されているログファイルを保全することは重要である．ログファイルは不正アクセスを受けた際に証拠として提出されるからである．法的証拠として利用する為にはアクセスログを改竄されていない状態で保全するシステムを組織的に業務に組み込んで運用する必要がある．提案システムは仮想計算機モニタを利用しているため，クライアント環境での利用の他にも，クラウドコンピューティング環境で実行されるサーバ用途へも適用可能である．

コンピュータフォレンジックスの性質上，コンピュータで扱う全てのデータを保全の対象とすることが理想的だが，頻繁に書き換えられるシステム関係のデータを対象としてしまうと，保全に必要とされる補助記憶装置の容量が膨大になってしまう．一方，ログファイルは基本的に追記のみを行うため，容量の問題が起きにくい特徴がある．本課題での提案はシステム領域を含むすべてのディスクに対する履歴保全が可能な設計を目指している．しかし，現段階では性能面を考慮し，第一ステップとしてログファイルのみを対象とした保全と回復のシステムの実現を目指して設計と実装を行うものとした．

２．研究の目的

本課題で開発したシステムでは，仮想計算機モニタ上で動作する OS が補助記憶装置へ書き込もうとした時に，データの書き込み時刻とデータを全て保全する．保全したデータを分析する際には，指定された時刻をパラメータとして与えて補助記憶装置の状態を復元する．同時に複数の時刻の状態を比較し，補助記憶装置に対して行われた操作履歴を調査できるシステムを目指す．加えて，仮想計算機モニタを用いることで，攻撃者に保全データを改竄・削除される可能性を低くする．

通常の補助記憶装置では，既に情報が書き込まれた領域に対して書き込みを行うと，古い情報は上書きされて消えてしまい，証拠として利用できなくなってしまう．通常の犯罪捜査ではハードディスクを押収し（データの保全），データの複製を作成して解析を行っている．ファイルシステム上で消去されたデータを復元するために専用ソフトウェアを用いてファイルシステムのメタデータやセクタに残っている上書きされていないデータをもとに，可能な限りの類推により削除されたデータを復元する．同一セクタに新しいデータが上書きされない限り，ある程度のデータ復元は可能であるが，完全に該当セクタが上書きされてしまうと，以前にあったデータの復元は通常の解析方法では不可能である．本提案では保全対象を仮想化されたハードディスクのイメージファイルとする．更に，仮想化の特性を活かして，書き込みを行う場合にも古い情報を削除せず，古い情報を残して情報を保全する機能を保全システムに組み込むものとした．保全する情報には時刻情報を付与し，復元時に時刻を指定できるようにする．これにより犯罪者が証拠を改竄や削除した場合に，証拠データを復元できるようにする．

ディスクの状態の復元については保全データに付与された時刻情報を参照し，指定された時刻の状態を示す情報を選択して読み出す．分析時には，複数の時刻の状態を復元して比較を繰り返すことで，情報が改竄された時刻を特定できる．また，改竄される前の状態を復元することもできる．

３．研究の方法

研究成果（１）　仮想計算機モニタで動作する移植性の高いデジタルフォレンシックスモジュールの開発

目的のシステムを実現するため，本課題ではまず仮想計算機モニタとして BitVisor と Xen への実装を検討した．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．BitVisor は Microsoft のようなソースコードの公開されていないシステムに対して透過的にセキュリティ機能を強制する目的で開発された．現在，BitVisor はオープンソースで公開され，多くのセキュリティ研究の基盤プラットフォームとして活用されている．BitVisor へのフォレンシック機能の実装は，ディスクの入出力を行う仮想計算機のパ

ラパススルー形式のデバイスドライバからデータを取得し，ハッシュ値を計算するまでの試作を行った．しかしながら BitVisor への実装は通常のシステムコールを利用できず，OS の開発に近い難易度を持つため，本課題では，移植性を考慮しながら，まずは Xen で実装を行い，そのソースコードを BitVisor へ移植する計画を立てた．以降では Xen でのプロトタイプ実装と評価について報告する．

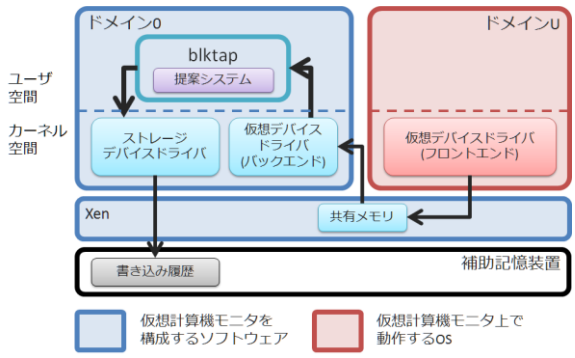

図１　システム構成

プロトタイプでは，Xen の準仮想化を利用し，blktap と呼ばれる仮想的なデバイスドライバで補助記憶装置への入出力を捕捉する機能を利用して実装を進めた．blktap は Xen のブロックデバイスへの入出力の処理を拡張するための仕組みである．Xen と blktap を利用したシステム構成を図１に示す．Xen では管理用の特殊な仮想計算機をドメイン 0，それ以外の通常の仮想計算機をドメイン U と呼ぶ．ドメイン U は，基本的にハードウェアに直接アクセスできないため，ドメイン U では，デバイスドライバの代わりにスプリットデバイスドライバのフロントエンドが動作しており，補助記憶装置への入出力要求は，Xen の共有メモリを通じてドメイン 0 にあるスプリットデバイスドライバのバックエンドに送られて処理される．blktap を利用する場合は，スプリットデバイスドライバのバックエンドに渡った要求がさらに blktap のデーモンプログラム（tap-ctl）に渡され，tap-ctl に組み込まれた tapdisk ドライバが実際の入出力処理を行う．tapdisk ドライバは，用途に応じて複数実装されている．仮想計算機モニタの起動時やマウント時に，使用する tapdisk ドライバを指定することができる．提案システムは Xen の blktap を利用した tapdisk ドライバとして実装し，保全する情報はドメイン 0 に保存するように実装した．

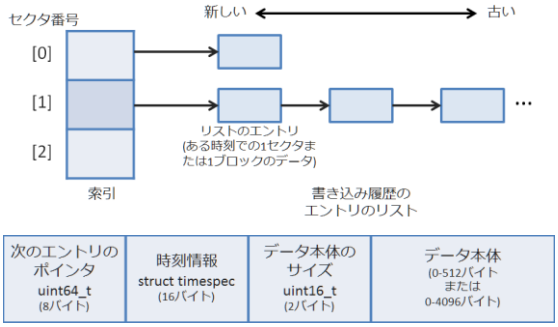

図２　履歴を保存するエントリの構造

履歴の保存は図２に示すエントリの構造体を作成し，それをブロックごとにリスト構造で保持することで実現した．また，別に索引ファイルも用意し，そこには各セクタ・ブロックのリストの先頭エントリ，すなわち最新のエントリのデータファイル上でのバイト単位の位置を保持する．索引ファイルからセクタ・ブロックの先頭のエントリの位置を取得することで，各セクタ・ブロックの最新の状態を取得でき，リストを辿ることで時系列順に過去のデータを探索できる．リスト構造のため追記が高速である．更なる高速化のために索引ファイルの内容はあらかじめメモリ上に展開しておき，読み込み時は索引ファイルにアクセスしないように実装した．

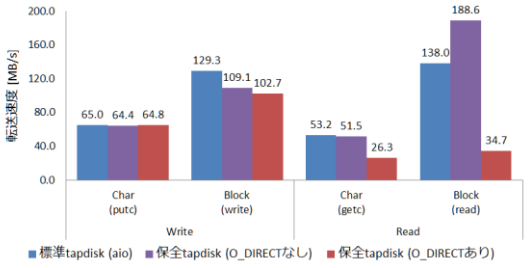

図３　プロトタイプの性能評価

補助記憶装置の入出力ベンチマークソフトウェアである bonnie++ 1.03e を利用し，保全機能を組み込んでいない標準の tapdisk ドライバ（aio）を利用する場合と，保全機能を組み込んだ tapdisk ドライバを利用する場合の入出力の速度を比較した．入出力速度の測定結果を図３に示す．Char は文字単位，Block はブロック単位での読み書きを評価した結果である．赤色の O_DIRECT ありはドメイン 0 での OS のディスク I/O キャッシュを無効にするオプションを採用したものであり，提案システムの実質的な性能を示している．

図３より分かるようにディスクへの書き

込みについては大きな性能低下は見られていない．しかしながら，読み込み時には文字列単位とブロック単位の両方の読み込みで性能が低下している．本システムが今回想定している運用方法は本稿の「１．研究開始当初の背景」で述べたとおりログファイルの証拠保全を行うことであった．ログファイルは基本的に書き込みしか発生しないため，性能が求められるのは主として書き込み性能である．読み込み性能は分析時に影響するが，分析時（犯罪捜査のために証拠を探す作業）はリアルタイム性は求められず時間をかけることができるためディジタルフォレンシックスシステムとしての実用性に関して大きく影響がでるものではないと考えられる．しかしながら実際の犯罪捜査では膨大なデータから証拠を探すことになるためシステムの性能を更に改善することが望ましい．

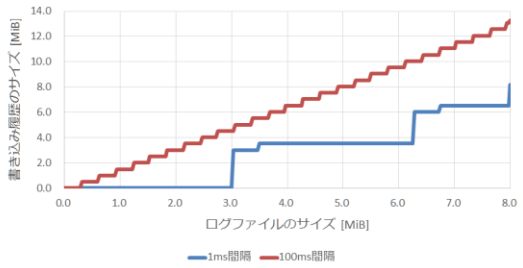

図４　履歴データのファイルサイズの評価

次に履歴データのファイルサイズについて調査を実施した結果を図４に示す．評価実験ではゲスト OS 側から，あるログファイルに対して，1［ms］間隔で 128 byte ずつ文字列を追記していった場合と，100［ms］間隔で 128 byte ずつ文字列を追記していった場合について，提案システム側の履歴データのファイルサイズを測定した．この結果，1［ms］間隔の場合はログファイルとシステムの履歴データが同一サイズであったのに対し，100［ms］間隔の場合には 1.65 倍にデータが増えた．これはゲスト OS 側のファイルシステムが fsync を一定時間ごとに実行してディスクにメモリ上のデータを書き込むため，履歴データ側のエントリが完全に埋まる前にリストが更新され，ディスクの利用効率が落ちることが原因であった．

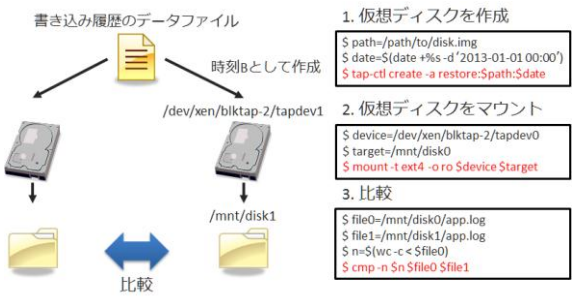

図５　開発したシステムの運用例

本課題で開発したシステムは Xen を用いて実装したため，サーバ側で仮想計算機モニタのレベルで特定のブロックデバイスを指定していおけば，そのブロックデバイスへの入出力履歴をすべて記録していき，任意時刻の状態のブロックデバイスをいつでも再現できるようになっている．これは MacOS の Time Machine の機能に似たものであるが，本課題で開発したシステムは，任意時刻の状態のディスクを同時にいくつでもマウントできる点が異なっている．この特徴により，例えば図５に示すように同時に２つの時刻のブロックデバイスをリードオンリーでマウントして，diff などの Unix ツールを用いて差分をとることができる．これを時系列に連続的に実行していくことでログの改竄があった時刻を突き止めることが可能となる．さらに本課題で開発したシステムは，任意時刻のブロックデバイスの状態を，ディスクのフォーマット(Ext4, NTFS, HFS+等)に関わらず再現することができる．これはシステムがブロック単位での入出力データをすべて記録しているからである．このため，提案システムを用いて特定時刻の状態を再現した分析用のリードオンリーの仮想ディスクを EnEase のような捜査機関が利用している市販ツールで解析することも可能となった．

本課題で開発したシステムは，性能面と容量面について更なる改善の余地があるものの，プロトタイプシステムとしては十分な性能を得ることができた．開発したソースコードは Xen に依存する部分は Blktap だけであり，Blktap も基本的にはブロック単位のデータを補足しているだけであるため，BitVisor への組み込みも大きな変更を伴わず実現できる見込みである．今後は BitVisor への組み込みを継続して実施していく計画である．

開発成果（２）：BitVisor へのロールベースアクセス制御システム（PERMIS）の組み込み

本課題での目的のひとつに企業等の組織において従業員のコンピュータ上での行動

（主として読み書きの記録）を監視するために仮想計算機モニタを利用することがあった．ディスクへの入出力の監視は研究成果（1）で示した Xen への実装でディジタルフォレンシックスのための基本モジュールを開発することができた．しかしながら，Xen は一般的にサーバ用途で利用される仮想計算機モニタであり，組織の個人が利用するコンピュータに導入する仮想計算機モニタを用いたセキュリティ基盤としては，BitVisor のほうが適している．特に BitVisor へ既に実装された国家公務員カード準拠の ID 管理機能を用いて，該当ユーザが扱ったデータを監視することが求められている．本課題ではこの目的を達成するため，ID 管理を発展させたロールベースアクセス制御（Role-based access control，略して RBAC）で実績のある PERMIS と呼ばれるソフトウェアを BitVisor へ組み込むための開発を実施した．

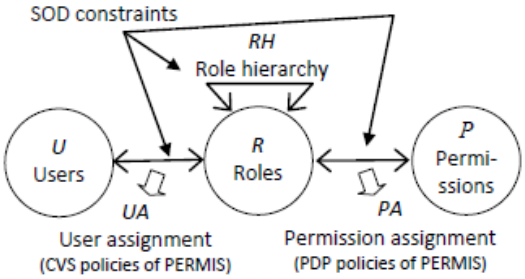

図６　ロールベースアクセス制御の仕組み

図６に セキュリティ基盤を構築するための仮装計算機モニタ BitVisor へ組み込んだロールベースアクセス制御の仕組みを示す．図６で User Assignment は IC カードに格納されたユーザの ID（公開鍵基盤における秘密鍵と公開鍵）を Role（役割）に割り当てるポリシーを示している．このポリシー（CVS Policy）は XML 形式のテキストファイルとして管理者が作成する．次に，Role（役割）を Permission（許可）に関連付ける Permission Assignment を実現するのが，PDP ポリシーと呼ばれる XML 形式で書かれたアクセス制御のテキストファイルである．BitVisor で RBAC 仕組みを実現するため，イギリスの University of Kent の David Chadwick 教授らが開発した PERMIS と呼ばれるソフトウェアを BitVisor へ組み込むための実装を行った．これにより BitVisor にて XML ポリシーでのアクセス制御を実現できるようになった．図７は実際に実装したシステムの基本設計である．IC カードから取得した ID を用いて，CVS ポリシーによりユーザと Role（役割）との関連付けを行い，PDP ポリシーによって最終的なアクセス制御を実現している．実装は PDP ポリシーを BitVisor のコンフィグレーションファイルに変換することで実現した．成果は「５．主な発表論文等」の〔学会発表〕（3）にて発表を行った．

～　セキュリティ基盤としての仮装計算機モニタ BitVisor へのディジタルフォレンシックス機能の組み込みに向けて　～

本課題では（1）Xen で開発したディジタルフォレンシクス機能を実現するモジュールと（2）BitVisor への RBAC モジュールの組み込み，の２つシステムの開発を実施した．開発成果(1)はディジタルフォレンシックスの基本機能を提供するモジュールである．開発成果(2)はディジタルフォレンシックスを適用するかどうかの判定に利用するためのものである．例えば，どの Role（役割，たとえば組織での職種や職位）を持つユーザが，どのブロックデバイスに，どのような日時にアクセスした際に，履歴保存の機能を適用させるべきかを判断する部分に活用できる．開発成果(2)についてはフォレンシックス以外の目的でも BitVisor を組織で活用する際に利用できるように実装をおこなった．

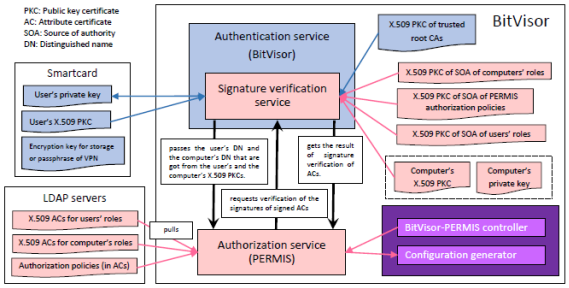

図７ BitVisor への RBAC の組み込み
（システム設計図）

４．研究成果

本課題の目的は仮想計算機モニタを拡張して Computer Forensics 分野へ適用を試みることであった．本課題で開発した成果(1)ディジタルフォレンシックスの基本モジュールは，紛争時や犯罪発生時に，電子的な証拠を安全に管理するための基盤として活用することが期待できる．さらに，開発成果(2)の BitVisor へのロールベースアクセス制御機能の組み込みによって，BitVisor を用いて組織内のコンピュータを効率的に管理することが可能となった．

開発成果（１）についてはホームページ（http://133.85.142.2/wiki/projects/hiranolaboratory/Hirano_Laboratory.html）にてソフトウェアを公開した．

本課題は２年間にわたり実施した．まず，初年度の平成２３年度は Linux のファイルシステムである ext4 の Digital Forensics

解析手法について検討した．さらにBitVisor のパラパススルードライバから入出力データを補足してハッシュ値を計算する試作を実施した．平成２４年度（最終年度）は仮想計算機モニタ Xen にてディジタルフォレンシックスの基本機能を実装した．本課題では，仮想計算機モニタのレベルでファイルシステムを解釈せず，ディスクへの入出力データをブロック単位で記録しておく手法を採用した．この結果，解析時に既存のフォレンシックスツールを用いること，既存 OS にマウントして Unix ツールを用いた解析を行うこと，が可能となった．更に，特定のファイルシステムに依存せず，原理的には Linux や Windows などの OS に対応できるものが開発できた．開発したフォレンシックスの基本モジュールは，Xen 依存の実装を避けたため，BitVisor への移植が容易となる設計となった．開発したモジュールによって，仮想計算機モニタで動作するゲスト OS のすべてのディスク入出力を時系列で記録することができるようになった．記録したデータは解析段階でシステムに日時を指定することで，タイムマシンのように，指定したディスクの状態をリードオンリーの状態として再現（OS 上にマウント）できるようになった．このシステムを用いて，複数の日時の状態を持つディスクを次々と再現（マウント）していき，ファイルの差分をとることで，アクセスログの改ざん日時を特定するシステムを開発し実証実験をおこなった．

本課題では上記に加えて，BitVisor へのロールベースアクセス制御の組み込みを行った．これにより，上記のフォレンシックスモジュールを活用する際に，利用者の ID だけではなく組織での役割（職種や職位）に基づいたデータ管理，電子的な証拠データの履歴の保存を行うための基本システムを作ることができた．

５．主な発表論文等

〔学会発表〕（計３件）

(1) Manabu Hirano, David W Chadwick, Suguru Yamaguchi, Use of Role Based Access Control for Security-purpose Hypervisors, The 5th IEEE International Workshop on Security in e-Science and e-Research (ISSR 2013), Melbourne, Australia , 16 - 18 July 2013. （採録決定）

(2) 小川拡，平野学．仮想計算機モニタを利用したコンピュータフォレンジックスのための補助記憶装置のデータの保全と回復のシステム．情報処理学会第 61 回コンピュータセキュリティ，第 21 回インターネットと運用技合同研究発表会，Vol.2013-CSEC-60 No.16, 3 月 14 日 2013.

(3) Manabu Hirano, Hiromu Ogawa, Takeshi Okuda, Eiji Kawai, Youki Kadobayashi, and Suguru Yamaguchi. A Digital Forensics System Using a Virtual Machine Monitor Integrated with an ID Management Mechanism. In USENIX Security Symposium 2011 Poster session, San Francisco, CA, USA, 11 August 2011.

〔その他〕
ホームページ等
研究成果(1)のソースコードの一般公開：
http://133.85.142.2/wiki/projects/hiranolaboratory/Hirano_Laboratory.html
上記ＵＲＬから本プロジェクトにて開発したソフトウェアのソースコードをダウンロードできます．

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