科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月　 ２ 日現在

機関番号：１２６１２
研究種目：若手研究(B)
研究期間：2011～2013
課題番号：２３７０００３２

研究課題名（和文）ハイパバイザの新しい応用の開拓

研究課題名（英文）Development of Novel Applications of Hypervisors

研究代表者
大山　恵弘（Oyama, Yoshihiro）

電気通信大学・情報理工学（系）研究科・准教授

研究者番号：１０３６１５３６

交付決定額（研究期間全体）：（直接経費）　　2,900,000円、（間接経費）　　870,000円

研究成果の概要（和文）：ハイパバイザの新しい応用を開拓した．世界に必ずしも普及していないが潜在的に有用なハイパバイザベースシステムを見出した．開拓した第一の応用は仮想マシンのデスクトップ画面へのメッセージ表示である．改造ハイパバイザがグラフィクスハードウェアのフレームバッファを操作し，画面上に画像を表示する．第二の応用は，プログラムコードに含まれる知的所有権保護である．OSカーネルのコードを公開部と秘密部に分割する．公開部は仮想マシンユーザに配られ仮想マシン内で実行される．秘密部は仮想マシンユーザから隠されハイパバイザにより実行される．クラウド計算やマルウェア検知の分野へのハイパバイザの応用についても研究を行った．

研究成果の概要（英文）：We have developed novel applications of hypervisors. We have identified several hypervisor-based systems that are not necessarily widespread in the world but are potentially useful. The first application we develop is to display messages on a desktop screen of a virtual machine. Our modified hypervisor manipulates the frame buffer of graphics hardware and thus displays images on the screen. The second application is to protect the intellectual properties included in program code. The application divides the code of an operating system kernel into a public part and a secret part. The public part is distributed to the users of a virtual machine and executed in the virtual machine. The secret part is hidden from the users of the virtual machine and executed by the hypervisor. We have also explored to apply hypervisors to the fields of cloud computing and malware detection.

研究分野：総合領域

科研費の分科・細目：情報学

キーワード：ハイパバイザ　仮想マシンモニタ　オペレーティングシステム　システムソフトウェア

１．研究開始当初の背景

ハイパバイザとは，計算機のハードウェアを仮想化し，上位層のソフトウェアに対して仮想的な計算機（仮想マシン, VM）を提供するためのソフトウェアである．ハイパバイザにより，単一の計算機上で複数の OS を動作させることや，ハードウェアと OS の間に新たなソフトウェア層を挿入することができるようになる．研究開始当初より，ハイパバイザは世界中で利用されていた．著名なハイパバイザとしては VMware Workstation, Xen, KVM, Microsoft Hyper-V などがある．

研究開始当初，ハイパバイザが利用される応用分野は，主に以下の 3 つであった．

(1) サーバ統合

複数の計算機上で運用していたサーバを，1 台の計算機上で運用するという応用である．ハイパバイザにより 1 台の計算機上に多数の VM を立ち上げ，各 VM 上で OS とサーバを動作させる．これにより，必要な計算機の数が減り，サーバ運用のコストを減らすことができる．近年注目されているクラウドコンピューティングでも，ハイパバイザによるサーバ統合が鍵技術となっている．

(2) ソフトウェア開発

ハイパバイザが提供する VM 上に様々な種類の OS や様々な設定のソフトウェアを動作させ，ソフトウェアの開発やテストを行うという応用である．ソフトウェア開発においては，しばしば，様々な OS や設定に対して動作確認や移植作業を行う必要がでてくる．その際, 各 OS や設定ごとに計算機の準備や OS のインストールを行うと，多大な人的，金銭的コストがかかる．

(3) 安全性および信頼性の強化

OS の下で動作するハイパバイザが，コンピュータウィルスなどのマルウェアの検査や，メモリやディスク上のデータの複製を行うという応用である．この応用のための技術は近年急速に発展し，現在では商用製品にも取り入れられている．

研究開始時におけるハイパバイザに関する研究の大半は，上記の応用分野のための技術を深化させるものであった．実際，それらの応用は実用的に成功しており，研究成果が社会に大きな価値をもたらしてきた．しかし，多くの研究者が長期間に渡り研究を行った結果，それらの技術は成熟段階に入り，革新的な変化をもたらす技術は出にくくなっている．

一方，他の応用分野に適用する視点からハイパバイザを見直すと，様々な新規技術を開発できる余地があることに気づく．

２．研究の目的

本研究の目的は，ハイパバイザの新しい応用分野の開拓である．本研究の動機は，ハイパバイザの「仮想的なハードウェアの提供」という性質を利用すると，今までほとんど顧みられなかった応用分野を切り拓ける可能性があるということである．本研究では，現在の主流以外の新しい応用を提案し，その有用性を示すことを目指した．

３．研究の方法

まず，オペレーティングシステム（OS）に依存しない形で画面にメッセージを表示するという応用と，プログラムコードに含まれる知的所有権を保護するという応用の 2 つを中心に技術開発を行った．他にも，必要に応じて，クラウド分野やセキュリティ分野において新しい応用を見出すことにも取り組んだ．本課題では実際にハイパバイザソフトウェアを開発し，実験による評価を通じて，それらの応用が有用であることを示すことを重視した．メッセージ表示システムについては，シンポジウムやワークショップなどにおいてデモを交えた発表を行い，視覚的にインパクトのある形で成果を世間に伝えることとした．

メッセージ表示に関しては，広告や警告などへの応用を検討し，実際にシステムを開発して性能などを評価した．既存のハイパバイザである BitVisor および KVM を改造する形でシステムの実装を行った．第一に，ユーザの入力や操作に合わせて，適切なメッセージを表示する技術を開発した．第第二に，メッセージを表示するタイミングや場所を賢く判断する技術を開発した．第三に，ユーザにメッセージの印象を強く与えるために，メッセージの文字や画像を移動させながら表示する技術を開発した．実装したシステムが実行時間に与える影響を実験により測定した．

メッセージ表示の具体的な実装方式は以下の通りである．BitVisor においては，ハイパバイザが直接実際のグラフィクスハードウェアの内容を書き換えることによって実現する．KVM においては，KVM が利用している QEMU の仮想グラフィクス処理部分を改造し，仮想グラフィクスハードウェアの内容をハイパバイザの指示で書き換えられるようにすることによって実現する．

プログラムコードに含まれる知的所有権の保護に関しては，ハイパバイザを利用して，OS カーネルのバイナリコードのうち公開したくない部分を, OS のユーザに渡さないようにしつつ，かつ，正常に実行させることを実現した．また，アプリケーションコードについても，一部をハイパバイザで実行するための機構の基本設計を行った．

OS カーネルのバイナリコードの知的所有権保護に関しては，Linux カーネルの命令列を秘密部と公開部に分離し，ハイパバイザ上で実行できるようにするシステムを実装し

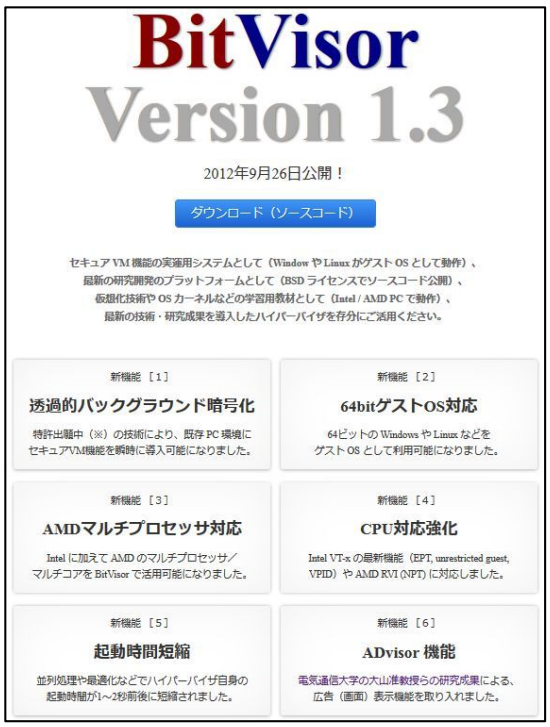
た．ハイパバイザの管理者は秘密部の情報をハイパバイザに格納し，ハイパバイザ上で動作する OS からは隠蔽する．OS が秘密部の命令列を実行する必要がある際には，自動的に OS からハイパバイザへと制御が遷移し，ハイパバイザが OS の代わりに命令を実行する．

その他の応用，たとえばクラウド分野やセキュリティ分野における新しい応用に関しても開拓を行った．

４．研究成果

メッセージ表示と知的所有権保護を中心に，マルウェアの検知や抑止も含めた，ハイパバイザの様々な応用を開拓した．応用のアイデアを示すのみならず，実際に動くシステムを作り，それを世界に向けて公開したり，性能評価をしたりした．

メッセージ表示の研究に関しては，本研究課題の成果が，世界的に利用されているハイパバイザである BitVisor に採用され，広く知られることになった．以下は BitVisor 公式ホームページに本研究課題の成果が述べられている図である．本研究のシステムの名称である「ADvisor 機能」という文言および研究代表者の名前が記載されている．



BitVisor に ADvisor 機能が入ったことは Web ニュースでも大きく報じられた．例えば詳細が以下のニュースに述べられている．

・Security NEXT.「国産 OSS セキュア VM の最新版「BitVisor 1.3」が公開 － 初期導入が容易に」，2012 年 9 月 28 日．http://www.security-next.com/034074

メッセージ表示のためのハイパバイザについては，メッセージを表示するという基本機能に加えて，様々な追加機能をシステムに組み込むことができた．まず，ネットワーク通信機能が加わった．具体的には BitVisor に UDP 通信機能を組み込み，画像を外部サーバから提供できるようにした．また，外部ホスト側で入力した文字をゲスト OS 上に表示する機能も加わった．これらにより，実用性が大きく上がったと考えている．

知的所有権保護に関しては，Linux カーネルの命令列を秘密部と公開部に分離し，ハイパバイザ上で実行できるようにするシステムを実装した．コードの分離に際しては，命令単位で命令を選択して秘密にする方式と，ブロック単位で秘密にする方式の両方を実装し，性能などを比較した．対象とするハイパバイザは，まずは，自身で一から開発した小さい実験用のものとした．

ゲスト OS 上で実行されるアプリケーションプログラムに含まれる知的所有権を保護するための研究も行った．その研究の技術は，アプリケーションプログラムの一部のコードをゲスト OS 側からハイパバイザ側に移すという技術を提案するものである．その成果をシンポジウムにおいて発表したところ，その発表が賞を受賞した．

ハイパバイザをセキュリティに応用する技術の重要性が高まったため，セキュリティ分野への応用を開拓する研究も行った．具体的には，ハイパバイザ層でマルウェアをシグネチャマッチングにより検知する技術の一層の深化を行った．この研究により，まず，ハイパバイザに組み込むマルウェアシグネチャ情報を，ハイパバイザや OS を止めることなく動的に更新できるようになった．また，ストレージの I/O データだけではなくメモリデータに対してもシグネチャマッチングができるようになった．本技術を利用して実際のマルウェアを検出するという実験も行い，有効性を評価した結果を論文で発表した．

正規表現で書かれたマルウェアシグネチャを用いるための技術の構築や，より多くの現実的なマルウェアを検知する実験を行うなどの研究成果も出した．

セキュリティ分野への応用として，ハイパバイザ層でパスワードクラッキングなどの悪意あるプログラム挙動を検出する技術の構築も進めた．実際に世界で広く用いられているパスワードクラッキングソフトウェアを用いて予備実験を行い，検出ができる可能性を認識した．

さらに，実ハードウェアに非常に似た仮想マシンを提供するハイパバイザ上でゲスト OS の実行状態の保存と復元をしながら，マルウェアの動的解析を行うシステムも構築した．従来の多くのハイパバイザでは仮想ハードウェアをゲスト OS に提供するため，マルウェアがハードウェアの動作を調べればハイパバイザの存在を容易に検知できるとい

う問題があった．本研究のハイパバイザでは，ゲスト OS からも実ハードウェアの動作が観測されるため，マルウェアによるハイパバイザの検知がより難しい．本研究では，Windows や Linux などの実用的な OS の実行状態を実際に保存，復元可能であることを確認した．

５．主な発表論文等

〔学会発表〕（計 15 件）

① 本田 惇，高橋 一志，大山 恵弘．“システムコールフックを用いた仮想マシン上のマルウェア検知と抑止”．第 11 回 ディペンダブルシステムワークショップ (DSW 2013)，熱海，2013 年 12 月．
② 河﨑 雄大，大山 恵弘．“BitVisor のための OS の状態復元機能”，第 11 回 ディペンダブルシステムワークショップ (DSW 2013)，熱海，2013 年 12 月．
③ 本田 惇，高橋 一志，大山 恵弘．“システムコールフックを用いた仮想マシン上のマルウェア検知と抑止”，第 25 回コンピュータシステム・シンポジウム (ComSys2013)，芝浦工業大学，2013 年 12 月．
④ 平井 成海，高橋 一志，大山 恵弘．“仮想マシンモニタによるプログラムコードの秘匿化”，第 25 回コンピュータシステム・シンポジウム（ComSys2013)，芝浦工業大学，2013 年 12 月．（学生ポスター賞受賞）
⑤ 三浦 俊朗，本田 惇，高橋 一志，大山 恵弘．“仮想マシンモニタによるパスワードクラッキング検出”，先進的計算基盤システムシンポジウム SACSIS 2013 論文集，pages 51-55，仙台，2013 年 5 月．
⑥ 河﨑 雄大，大山 恵弘．“BitVisor のためのマルウェアの検出機能”，BitVisor Summit，東京，2012 年 12 月．
⑦ 大山 恵弘，河﨑 雄大．“BitVisor を用いたメッセージ表示システム”，BitVisor Summit，東京，2012 年 12 月．
⑧ Yoshihiro Oyama．“Hypervisor-Based Systems for Malware Detection and Prevention”，NSC-JST Workshop on "Information and Communication Technology" 2012, Tokyo, November 2012. http://www.jst.go.jp/sicp/ws2012_nsc.html
⑨ 大山 恵弘，河﨑 雄大．“ハイパバイザ内シグネチャマッチングによるマルウェア検出”，マルウェア対策研究人材育成ワークショップ 2012 (MWS 2012)，pages 122-129，松江，2012 年 10 月．
⑩ 河﨑 雄大，大山 恵弘．“VMM を用いたマルウェア検出システムのためのシグネチャデータ更新機能とメモリデータ検査機能”，情報処理学会 2012 年並列／分散／協調処理に関する『鳥取』サマー・ワークショップ（SWoPP 鳥取 2012），7 pages，鳥取，2012 年 8 月．
⑪ Keisuke Okamura，Yoshihiro Oyama．“Controlling the Speed of Virtual Time for Malware Deactivation”，In Proceedings of the 3rd ACM SIGOPS Asia-Pacific Workshop on Systems (APSys 2012), Seoul, Korea, July 2012. DOI: 10.1145/2349896.2349902
⑫ 佐久間 充，大山 恵弘．“HyperCensor: 仮想マシンモニタを用いた OS バイナリコードの秘匿化”，ディペンダブルシステムワークショップ＆シンポジウム（DSW & DSS 2011），8 pages，京都，2011 年 12 月．
⑬ 小川 夏樹，大山 恵弘．“ADvisor: ゲスト OS の操作に連動した広告を表示するハイパバイザ”，情報処理学会 2011 年並列／分散／協調処理に関する『鹿児島』サマー・ワークショップ（SWoPP 鹿児島 2011），7 pages，鹿児島，2011 年 7 月．

〔その他〕
ホームページ等
http://www.ol.inf.uec.ac.jp/
http://www.ol.inf.uec.ac.jp/research/advisor/

６．研究組織

(1)研究代表者

大山 恵弘（OYAMA, Yoshihiro）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：10361536