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　１６　日現在

機関番号：　１２１０２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３００８０

研究課題名（和文）安全と安心を提供するための先進的ハイパバイザ技術

研究課題名（英文）Advanced hypervisor technology to provide safety and security

研究代表者
大山　恵弘（OYAMA, Yoshihiro）

筑波大学・システム情報系・准教授

研究者番号：１０３６１５３６

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：安全と安心を提供するための先進的ハイパバイザ技術を構築した．ハイパバイザがコンピュータのデスクトップ画面に災害警報などのメッセージを表示するための基盤技術を開発した．ハイパバイザ層でマルウェアの検知と無力化を行うための要素技術や，マルウェアを効率的に解析するためのハイパバイザも開発した．また，近年収集されたマルウェアを詳細に分析し，洗練されたマルウェアが解析に対抗するために実行する処理を明らかにした．さらに，マルウェアの動作ログを文脈自由文法を用いてコンパクトに保存するための技術を開発した．マルウェアの挙動のうち特にスリープ処理に関係するものについての調査と実験も行った．

研究成果の概要（英文）：We developed advanced hypervisor technologies to provide safety and security. We developed a fundamental technology with which a hypervisor displays messages such as disaster warnings on the desktop of a computer. We also developed an elemental technology to detect and disable malware in the hypervisor layer and a hypervisor for efficient malware analysis. Moreover, we analyzed recently collected malware samples and clarified the operations executed by sophisticated malware to countermeasure analysis. Furthermore, we developed a technology to store malware behavior logs compactly using context-free grammar. We also conducted investigation and experiments on malware behavior particularly related to sleep operations.

研究分野：　システムソフトウェア

キーワード：　ハイパバイザ　仮想化　仮想マシンモニタ　災害警報　マルウェア　セキュリティ　安心　オペレーティングシステム

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．今日，ハイパバイザは世界中で利用されている．著名なハイパバイザとしては VMware，Xen，KVM，Hyper-V などがある．ハイパバイザが利用される応用分野は，主に以下のものである．

(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．近年著しい発展を遂げたクラウドコンピューティングにおいても，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) 信頼性の向上
OS の下で動作するハイパバイザがメモリやディスク上のデータの複製を行うことや，その複製をもとにその OS を別の計算機上で動作させることにより，サーバなどの信頼性を向上させる応用である．この応用のための技術も，近年急速に発展している．

ハイパバイザに関する既存研究の大半は，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いる．しかし，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，人々に安全，安心を提供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．

２．研究の目的

安全と安心を提供するための先進的ハイパバイザ技術を構築する．具体的には，災害警報のメッセージを画面に表示する機能を提供するハイパバイザ，および，マルウェアの検知と無力化の機能を提供するハイパバイザの実装手法を確立し，実際にハイパバイザを試作する．さらに実験によりそれらのハイパバイザの有用性を評価する．メッセージ表示機能は，画面情報が格納されたメモリ領域（フレームバッファ）を OS とは独立にハイパバイザが書き換える，またはハイパバイザが主導的に GPU を操作することにより実現する．マルウェア検知の機能は，OS のメモリ上データ，転送されるディスクブロック，通信されるネットワークパケットなどの重要データをハイパバイザが監視することにより実現する．マルウェア無効化の機能は，仮想ハードウェアの動作を変更することや，ディスクブロックなどのデータの中身を書き換えることにより実現する．どの機能についても，既存のハイパバイザを拡張して実装し，成果が実用的なものになることを狙う．

３．研究の方法

メッセージ表示機能に関しては，まず，ハイパバイザがデスクトップ画面にメッセージを表示するための基盤技術を開発する．それはハイパバイザ層でグラフィクスハードウェアを直接操作することにより実現する．本研究で実装するハイパバイザは，OS とビデオハードウェアとのやりとりを捕捉し，画面情報が格納されたメモリ領域（フレームバッファ）をメッセージが表示されるように改変することにより実現される．並行して，ハイパバイザが OS の助けを借りずに外部サーバと通信するための技術を開発する．

次に，ハイパバイザが地震などの災害情報を提供するサーバから情報を実際に取得し，災害情報をユーザが気づきやすい形でディスプレイ上に表示する機構を開発する．そして，その機構の設計方式，実装方式，有用性を明らかにする．

マルウェアの検知と無力化の機能に関しては，アプリケーションが処理しているデータや外部との間の通信データを解析してマルウェアを検知する．さらに，マルウェアに限らず，脆弱なプロトコルによる通信などのデータも検知できるようにする．また，ハイパバイザを改造して仮想タイマハードウェアの動作を変更し，プロセスを制御することも検討する． マルウェアが時間管理に関して実行する処理についても調査し，それをマルウェアの検知や制御に役立てる．

研究にあたっては，オープンソースのハイパバイザである BitVisor と KVM をもとに開発や実験を行う．ハイパバイザ上で動かす OS としては，Windows と Linux を想定する．CPU としては Intel アーキテクチャのうち VT 機能を有するものを対象にする．

研究成果は論文や学会発表の形で社会・国民に発信する．さらに，成果物のソフトウェアをオープンソース公開する．Web を通じた成果公開も行う．

４．研究成果

安全と安心を提供するための先進的ハイパバイザ技術を構築した．まず，ハイパバイザがコンピュータのデスクトップ画面にメッセージを表示するための基盤技術を開発した．その技術は，ハイパバイザがゲスト OS とは独立にグラフィクスハードウェアを直接操作するものや，外部サーバと直接通信するものからなる．災害情報を提供するサーバとインターネットを介して UDP/IP により通信してディスプレイに災害警報を表示するシステムを実際に構築し，そのようなシステムをハイパバイザによって実現可能であることを示した．災害警報の情報は独自のプロトコルに従って送受信される．そのプロトコルでは，災害の種類やレベル，メッセージの内容などを指定できる．

マルウェアの検知と無力化や，安全と安心のためのシステムについても要素技術を開発した．まず，ハイパバイザ層でマルウェアを検知し，セキュリティポリシーに基いて様々な対策処理を適用するシステムを構築した．また，ディスクブロックやネットワークパケットをはじめとする様々なデータを収集し，OS にできるだけ依存しない形でハイパバイザがプログラムの動作を推定したり，プログラムの動作を制御したりする方式の設計も行った．安全性の低い SSL/TLS 通信をハイパバイザ層で検出し，ユーザへの通知や通信の遮断を実行するための技術を構築した．この技術では BitVisor を拡張してシステムを実装し，実験を通じて高い有効性を示した．ハイパバイザの利用によりオペレーティングシステムにほとんど依存しないセキュリティシステムが実際に構築できることを示した点に研究意義がある．実際，ハイパバイザの利用により実際に Windows と Linux の両方に対して安全性を高めることに成功している．

マルウェアを効率的に解析するためのハイパバイザも開発した．このハイパバイザは，実機と見分けることが困難である仮想マシンを提供し，かつ，その仮想マシンのチェックポインティングを可能にする．近年では仮想マシンの存在を検知して解析を妨害するマルウェアが多くなっている．このハイパバイザは，そのような仮想マシン検知を困難にできるため，マルウェアの解析を支援することができる．

ハイパバイザを用いて安全と安心を実現するための新しい方法も提案した．その方法では，ハイパバイザがデスクトップ画面を画像解析し，有害なコンテンツが表示されているかどうかを判断する．表示されていると判断した場合には，ハイパバイザは有害部分を黒塗りするなどしてユーザがそのコンテンツを見ることを妨げる．この方法により．青少年が有害な画像や情報に接することを保護者や教師が防止しやすくなる．この方法を BitVisor に統合したシステムを構築し，どの程度の性能とどの程度の精度で黒塗りができるかどうかを検証した．

近年の洗練されたマルウェアの動作を明らかにする研究も行った．それらのマルウェアでは，ハイパバイザの存在を検査し，もし存在する場合には，自身が解析環境で動作している可能性があると判断して実行を終了するなどの対策処理を実行する．そこで，近年収集されたマルウェアを詳細に分析し，それらが解析に対抗するために実行する処理を明らかにした．関連して，マルウェアの動作ログをコンパクトに保存するための技術を開発した．具体的には，文脈自由文法を利用したログ圧縮技術を開発し，その技術によってマルウェアの動的解析ログが高圧縮率で圧縮できることを示した．

マルウェアの時間に関する挙動のうち，特にスリープ処理の挙動についての調査と実験も進めた．自ら一定時間実行を休止するスリープ処理を近年のマルウェアがどう利用しているかを明らかにするとともに，スリープ処理の挙動を利用してマルウェアの分類や検知を行う方法の可能性を示した．

その他にも，ハイパバイザを用いて知的所有権を保護する技術や，ブラウザの拡張機能によって有害な Web コンテンツを自動的に認識して遮断する技術を開発した．

５．主な発表論文等

〔雑誌論文〕（計 4 件）

① 高橋 研介、市野 将嗣、大山 恵弘、ブラウザ拡張機能を用いた動的コンテンツフィルタリングシステム、情報処理学会論文誌、査読有、Vol.58、No.5、2017、pp.1175-1188
http://id.nii.ac.jp/1001/00178855/

② Takahiro Okumura, Yoshihiro Oyama, Grammar Compression of Call Traces in Dynamic Malware Analysis, Journal of Information Processing, 査読有, Vol.25, No.2, 2017, pp.229-233.
DOI: 10.2197/ipsjjip.25.229

③ Yoshihiro Oyama, Trends of anti-analysis operations of malwares observed in API call logs, Journal of Computer Virology and Hacking Techniques, 査読有, 2017-02.
DOI: 10.1007/s11416-017-0290-x

④ Yoshihiro Oyama, Yudai Kawasaki, Kazushi Takahashi, Checkpointing an Operating System Using a Parapass-through Hypervisor, Journal of Information Processing, 査読有, Vol.23, No.2, 2015, pp.132-141.
DOI: 10.2197/ipsjjip.23.132

〔学会発表〕（計 13 件）

① 大山 恵弘、マルウェアのスリープ挙動の多様性に関する予備調査、情報処理学会研究報告コンピュータセキュリティ、2017-CSEC-76(15)、2017、神奈川工科大学（神奈川県厚木市）
http://id.nii.ac.jp/1001/00178412/
② 大山 恵弘、マルウェアによる対仮想化処理の傾向についての分析、コンピュータセキュリティシンポジウム 2016 論文集、2016、pp.534-541、秋田キャッスルホテル（秋田県秋田市）
http://id.nii.ac.jp/1001/00175746/
③ 大山 恵弘、ハイパバイザによる災害警報通知システムの実装方式、日本ソフトウェア科学会第 33 回大会講演論文集、2016
④ 平井 成海、SSLWatcher: SSL/TLS 通信を監視し警告するハイパバイザ、BitVisor Summit 4、2015、お茶の水女子大学（東京都文京区）
https://www.bitvisor.org/summit4/
⑤ 宮本 景冬、ADvisor 機能を応用した有害画像の視覚的抑制、BitVisor Summit 4, 2015、お茶の水女子大学（東京都文京区）
https://www.bitvisor.org/summit4/
⑥ 高橋 研介、高橋 一志、大山 恵弘、ブラウザ拡張機能を用いた動的コンテンツフィルタリングシステムの提案、コンピュータセキュリティシンポジウム 2015 論文集、2015、pp.124-131、長崎ブリックホール（長崎県長崎市）
http://id.nii.ac.jp/1001/00146776/
⑦ 大山 恵弘、ハイパバイザによる災害警報通知、第 14 回情報科学技術フォーラム、2015、pp.213-216、愛媛大学（愛媛県松山市）
http://id.nii.ac.jp/1001/00153618/
⑧ 平井 成海, 高橋 一志, 大山 恵弘、SSLWatcher: SSL/TLS 通信を監視し警告するハイパバイザ、日本ソフトウェア科学会第 32 回大会、2015、早稲田大学（東京都新宿区）
⑨ Yoshihiro Oyama, A Hypervisor for Manipulating Guest Screens, In poster session in the 6th ACM SIGOPS Asia-Pacific Workshop on Systems, 2015, Tokyo (Japan).
http://www.sslab.ics.keio.ac.jp/apsys2015/program/
⑩ 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 12 回ディペンダブルワークショップ、2014, ホテル水葉亭（静岡県熱海市）
⑪ Yoshihiro Oyama, Natsuki Ogawa, Yudai Kawasaki, Kazuhiro Yamamoto, ADvisor: A Hypervisor for Displaying Images on a Desktop, In Proceedings of the 2nd International Symposium on Computing and Networking, 査読有, 2014, pp.412-418, Shizuoka (Japan).
DOI: 10.1109/CANDAR.2014.43
⑫ 本田 惇、高橋 一志、大山 恵弘、仮想マシンモニタによるマルウェアプロセスの実行抑止、日本ソフトウェア科学会第 31 回大会、2014、名古屋大学（愛知県名古屋市）
⑬ 平井 成海、髙橋 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、2014 年並列／分散／協調処理に関する『新潟』サマー・ワークショップ（SWoPP 新潟 2014）、2014、新潟コンベンションセンター（新潟県新潟市）
http://id.nii.ac.jp/1001/00102327/

〔その他〕
DisasVisor ソフトウェア公開 Web ページ
https://github.com/y-oyama/DisasVisor

６．研究組織

(1)研究代表者
大山 恵弘（OYAMA, Yoshihiro）
筑波大学・システム情報系・准教授
研究者番号：10361536