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　５ 年　 ６ 月　 １ 日現在

機関番号：５７１０２
研究種目：若手研究
研究期間：2019～2022
課題番号：１９Ｋ２０２４６

研究課題名（和文）未知の攻撃に遭遇した際のプロセスの振る舞い検知と解析に関する研究

研究課題名（英文）A Study on Detecting and Analyzing Unidentified Cyber Attacks through Process Behavior Examination

研究代表者
森山　英明（Hideaki, Moriyama）

有明工業高等専門学校・創造工学科・准教授

研究者番号：００６３３００９

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：　コンピュータ上の重要なファイルを対象とした攻撃を検知し，振る舞いを解析する手法について提案を行った．提案に基づき，仮想計算機を利用して，仮想マシン(VM)上で動作するプロセスの振る舞いを監視する機構を実装した．具体的には，仮想マシンモニタ(VMM)上に監視機構を組み込み，プロセスの振る舞いを検知しログとして出力する．また，プロセスの振る舞い解析時の情報の漏えいを防ぐために，プロセス間通信処理に改良を加え，情報漏えいを防止する機能を実現した．さらに，監視による処理負荷の増加を抑えるため，ファイルパス取得処理とログ出力処理の改善を行い，この有効性を評価によって確認した．

研究成果の学術的意義や社会的意義
　クラウドコンピューティングやIoTによるサービスの増加に伴い，コンピュータ上の重要な情報を狙ったサイバー攻撃も増加し，攻撃の手口も巧妙化している．これに伴い，サイバー攻撃を防ぐための手法や技術が提案されているが，多くは既知の攻撃を対象としたものであり，ゼロデイ攻撃や標的型攻撃といった未知の攻撃に対する検知が困難である．本研究は，これらの未知の攻撃に対して自動的に攻撃を検知し振る舞いを分析する機構を提案したものであり，攻撃の検知システムの構築，振る舞いの解析環境の構築，および性能に関する考察を行うことで有用性を示した．

研究成果の概要（英文）：We proposed a method for detecting and analyzing cyber attacks targeting important files that contain classified information. Based on the proposal, we implemented a mechanism to monitor the behavior of processes running on virtual machines (VMs) using virtual machine monitors (VMMs). The monitoring mechanism detects process behavior triggered by system calls and records monitoring logs. To ensure data security during process behavior analysis, we improved interprocess communication processing to prevent information leakage. Additionally, we improved the file path retrieval and log output processes to reduce monitoring overhead. These improvements were validated through the evaluation of processing overhead.

研究分野：オペレーティングシステム

キーワード：オペレーティングシステム　仮想計算機　セキュリティ　振る舞い解析

１．研究開始当初の背景

近年，ネットワークによる通信の品質が向上したことで，多くの企業からネットワークを介した様々なサービスが提供されている．また，計算機性能の向上により，スマートフォンに代表される小型かつ高性能な携帯端末機が販売されており，多くの利用者によってネットワークを介したサービスが利用されている．今後，モノのインターネット化（IoT: Internet of Things）や自動車の自動運転システムの実用化が進むにつれて，人々の生命にかかわる重要な作業や判断をコンピュータにゆだねる可能性が出てくると考えられ，情報技術が社会に与える影響はますます大きくなると考えられる．このような環境において，サービスの提供に必要となるデータは，ネットワークを介して集約されるため，これまで以上に，個人に関する重要な情報がネットワーク上の脅威に晒される機会が多くなると考えられる．一方で，現在，重要な情報を扱う際に必要となるセキュリティに関しては，専門的な知識を持った管理者による対応が行われており，今後，膨大な量の個人情報をやり取りする上で対応しきれなくなると予想される．このため，外部からの攻撃を受けにくい堅牢なセキュリティシステムによる保護のサポート，自動化が必要である．

２．研究の目的

既存のセキュリティ技術では，未知のサイバー攻撃への対策が困難である．また，システム管理者は常に高いセキュリティを保つことが求められるが，人が手動で対処することは難しい．本研究では，多くのサービスが仮想計算機環境で提供されることに着目し，VM 上のプログラムの振る舞いを VMM から監視し，重要な情報へのアクセスがあった場合は，セキュアな検査環境を自動的に作り，振る舞いの検査と解析を行うことで，重要な情報の取得やデータの改ざんを防ぐシステムの実現を目指す．本手法では，システムコールを契機として解析を行うことから，未知の攻撃に対する解析が可能であること，VM に手を加えないことから適用範囲が広いという利点がある．

３．研究の方法

計算機仮想化技術を利用し，重要情報を対象とした未知の攻撃に対して自動的に保護と分析を行う機構を提案し，実現に向けた検討を行う．仮想計算機技術は，近年の計算機性能の向上により様々な場面で用いられるようになった技術で，ネットワークを用いたサービスの提供で多く利用されている．仮想計算機技術を利用したサービスの利用形態を図１に示す．ネットワークを介したサービスの利用者や前述の IoT におけるセンサは，物理計算機上に構築される仮想計算機（VM: Virtual Machine）上のアプリケーション（AP: Application Program）に対して，データの送受信を行う．各 VM の管理者は，サービスの安定した提供や，重要データの保護を行うために，常にシステムを最新の状態に保ち脅威に備えることで，高いセキュリティを保つことが求められる．しかし，ソフトウェアにおける脆弱性は日々見つかっており，また，近年では重要データの取得を目的とした標的型攻撃やゼロデイ攻撃といった，既存手法では対応しきれない脅威に晒されている．

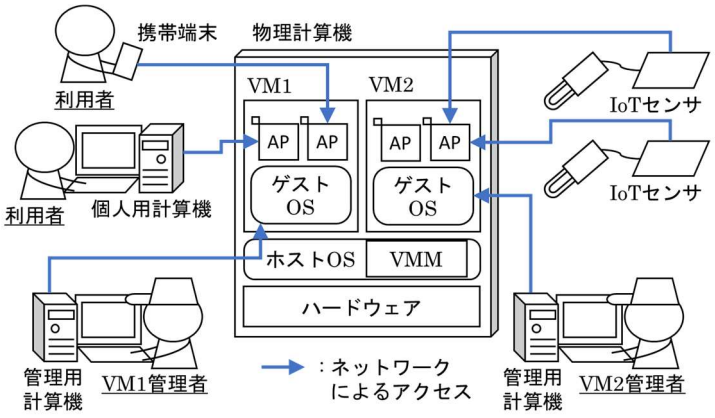

図１ 計算機仮想化技術を用いたサービスの利用形態例

そこで，本提案手法では，各 VM が VMM（Virtual Machine Monitor）によって管理されることに着目し，VMM 上に監視機構を実装し，VM 上のプロセスが重要な情報へのアクセスを試みた際に，処理を検知し防止する機構を実装する．

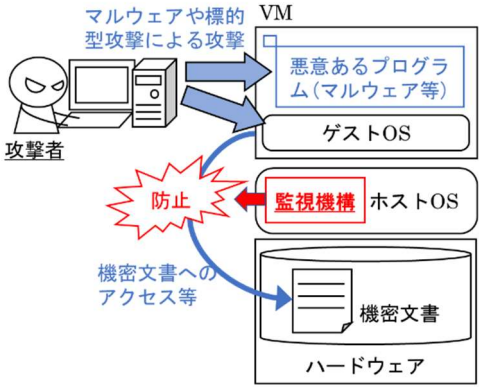

図２ 提案手法により攻撃を防止する様子

本提案手法により攻撃を防止する様子を，図 2 に示す．重要なデータを取得しようとする攻撃者は，攻撃対象の VM に対して，ネットワークを介してマルウェアなどの悪意あるプログラムを導入しようと試みることや，オペレーティングシステム（OS）の脆弱性を利用した標的型攻撃を行うことが知られている．本提案手法では，攻撃対象となる VM 上ではなく，ホスト OS

上の VMM に監視機構を実装することで，OS の脆弱性を利用されることによるデータ改ざんも防止可能であると考える．

４．研究成果

提案で述べた監視機構を実現するために，以下の 4 つの機能が必要であると考えた．

(1) ネットワークを介した情報流出を防止する機能：
攻撃者による外部への機密情報の拡散経路として，ネットワークを介した拡散が考えられる．このため，機密情報を有する可能性のあるプロセス（以降，管理対象プロセスと呼ぶ）が外部へ通信を行う際は，これを禁止する必要がある．

(2) 機密情報を扱うプロセス・ファイルの登録と振る舞いを記録する機能：
管理対象プロセスにより，プロセスやファイルの生成・変更の処理が実行される場合，これらの情報として機密情報が含まれる可能性がある．このため，監視機構により，これらを管理する必要のあるプロセス，ファイルとして登録し（以降，管理対象プロセス，管理対象ファイルと呼ぶ），振る舞いを記録する．

(3) 保全を考慮したバックアップの作成機能：
サイバー攻撃の中には，計算機システムのデータを変更することで，システムの正常な実行を阻害するものがある．振る舞いの解析を行う際に，誤ってこれらの処理の実行を許可しても，正常な VM の状態に戻すことが出来るよう，スナップショット機能等を用いて VM のバックアップを作成する．

(4) 問題ある一連の動作の自動通知機能：
多くのマルウェアは，一連の決まった振る舞いを行う．監視機構は，これまでに振る舞いを解析した結果を用いて自動的に攻撃を検知し，利用者への通知を行う．

以上の機能を持つ監視機構の実現方式について，提案を行った．以降，この監視機構を振る舞い解析機構と呼ぶ．振る舞い解析機構の構成を図 3 に示し，以下で説明する．

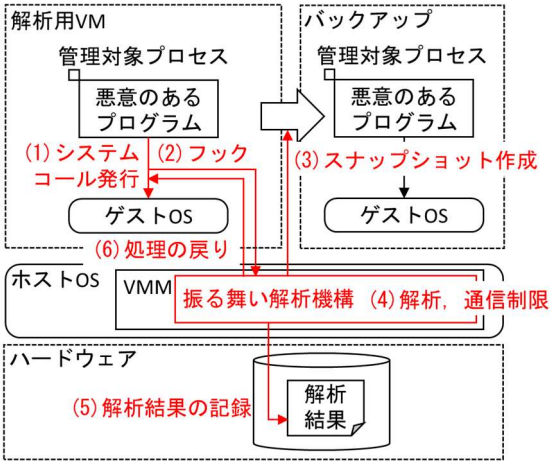

図 3 振る舞い解析機構の構成

VM 上のプロセスが処理を実行する際，正常な処理であるか攻撃に伴う処理であるか判断がつかない．このため，プロセスが発行するシステムコールに着目し，システムコールを契機とした解析を行う．具体的には，VM 上でシステムコールが発行される際（図 3 の(1)），VMM 上の振る舞い解析機構はシステムコールをフックし（図 3 の(2)），システムコールの処理を一時中断する．このとき，現在の VM 環境のバックアップとしてスナップショットを作成する（図 3 の(3)）．もし，システムコールが管理対象プロセスや管理対象ファイルと情報をやり取りする場合，システムコールを発行したプロセスを管理対象プロセスとして登録する．同様に，管理対象プロセスがファイルへ情報を書き出す場合，このファイルを管理対象ファイルとして登録する．管理対象プロセスが 1 個以上存在する間は，監視対象とする VM を解析用 VM として扱い，振る舞い解析機構から外部へのネットワークアクセスを制御した状態にする（図 3 の(4)）．システムコールの情報を取得し，これらの情報をプロセスの振る舞い情報として記録して（図 3 の(5)），処理を VM 側へ戻す（図 3 の(6)）．このとき，集約した振る舞いのログからマルウェア等の攻撃を特定した場合，利用者に警告を通知する．

提案した実現方式に対して，実装を行った．この実装により，「(1)ネットワークを介した情報流出を防止する機能」と「(2)機密情報を扱うプロセス・ファイルの登録と振る舞いを記録する機能」について実現した．(1)は，管理対象プロセスによるプロセス間通信処理において，ソケットへデータを転送するシステムコールやファイルディスクリプタ間でデータを転送するシステムコールが参照する VMCS(Virtual Machine Control Structure)の値を変更することで，情報の流出を防止する機能を実装し，通信の遮断が可能であることを確認した．(2)は，VM 上のプロセスからシステムコールが発行される際に，ハードウェアブレークポイントを用いて，システムコール発行(SYSCALL 命令)と終了(SYSRET 命令)時にデバッグ命令を発生する手法を用いて実装した．さらに，(2)の機能による処理の増加が懸念されるため，処理オーバヘッドの測定を行い，これを削減する手法を提案した．図 4 に示す read/write システムコールを用いた評価や，図 5 に示すファイルアクセスに関するベンチマーク fio を用いた評価により，オーバヘッド削減の有効性を明らかにした．

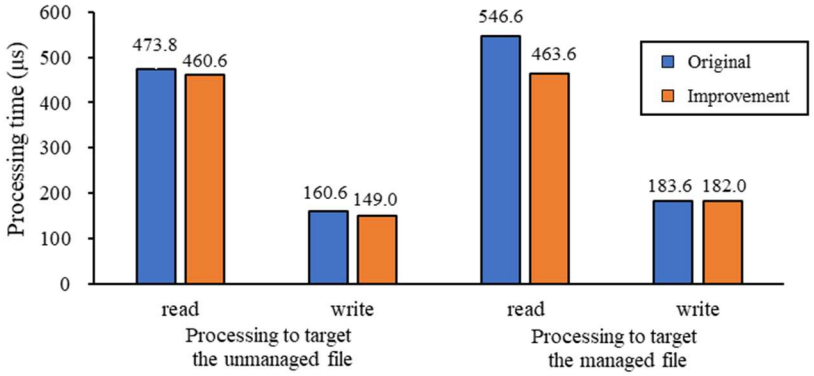

図 4　read/write システムコールを用いた処理時間の評価

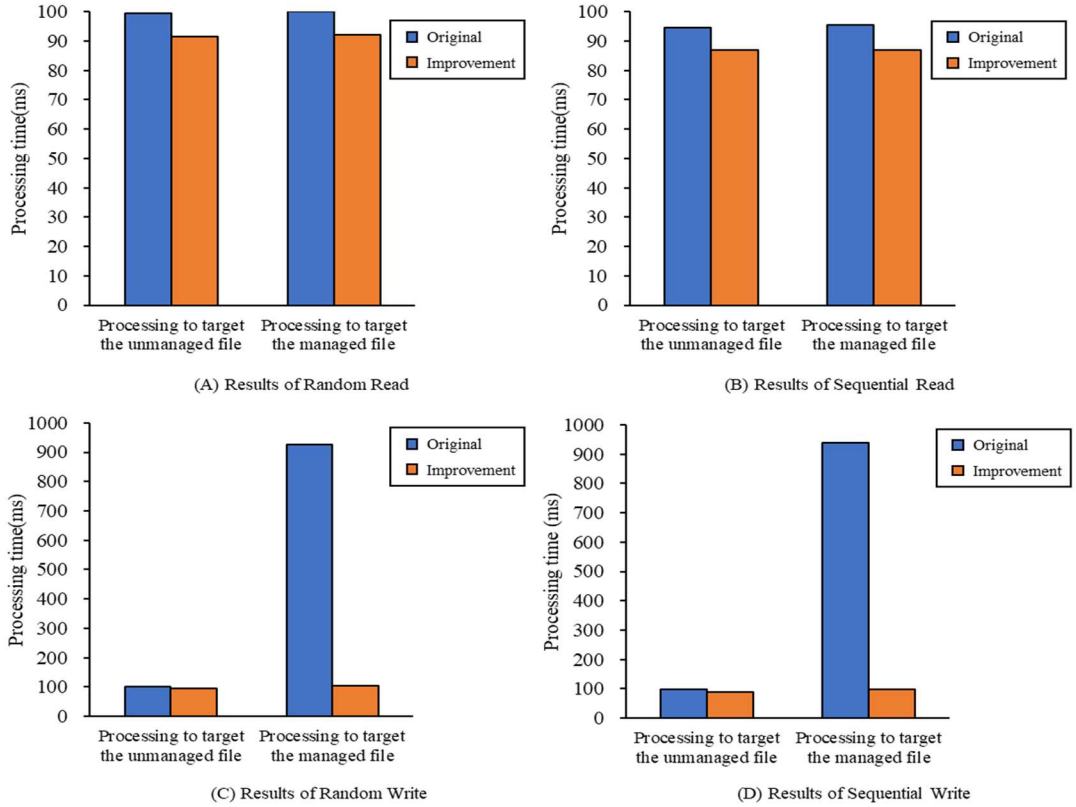

図 5　fio ベンチマークを用いた処理時間の評価

一方，「(3)保全を考慮したバックアップの作成機能」と「(4)問題ある一連の動作の自動通知機能」は課題が残っている．(3)において，システムコール処理発生時にスナップショットを取得することは処理オーバヘッドの観点から困難であると考え，VM 上のシステムコール処理の実行を阻害しない形での別のアプローチを検討している．(4)は，現在，システムコールを振る舞いとして管理していることから，システムコールの発行頻度や順番から攻撃の種類を推定する方法を検討しているが，対応付けが困難といった問題がある．この問題については，振る舞い解析機構による解析結果の数が不足していることが原因であると考えており，今後は様々なサイバー攻撃を対象として振る舞い解析の数を増やすことで，解決が可能であると考える．

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Hideaki Moriyama, Toshihiro Yamauchi, Masaya Sato, Hideo Taniguchi	４．巻 12
２．論文標題 Improvement and Evaluation of a Function for Tracing the Diffusion of Classified Information on KVM	５．発行年 2022年
３．雑誌名 Journal of Internet Services and Information Security (JISIS)	６．最初と最後の頁 26-43
掲載論文のDOI（デジタルオブジェクト識別子） 10.22667/JISIS.2022.02.28.026	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 森山 英明	４．巻 2020
２．論文標題 機密情報へのアクセスを解析する解析用VM作成手法の実現	５．発行年 2020年
３．雑誌名 電気・情報関係学会九州支部連合大会講演論文集2020	６．最初と最後の頁 211
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 本田 匠, 森山 英明	４．巻 2020
２．論文標題 プロセス間通信による機密情報拡散をKVMから防止する機能の検討	５．発行年 2020年
３．雑誌名 電気・情報関係学会九州支部連合大会講演論文集2020	６．最初と最後の頁 209 - 211
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 Moriyama Hideaki、Yamauchi Toshihiro、Sato Masaya、Taniguchi Hideo	４．巻 1264
２．論文標題 Improvement and Evaluation of a Function for Tracing the Diffusion of Classified Information on KVM	５．発行年 2020年
３．雑誌名 Advances in Networked-Based Information Systems, NBiS 2020, Advances in Intelligent Systems and Computing	６．最初と最後の頁 338～349
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-57811-4_32	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3件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 森山 英明
2．発表標題 機密情報へのアクセスを解析する解析用VM作成手法の実現
3．学会等名 電気・情報関係学会九州支部連合大会
4．発表年 2020年

1．発表者名 本田 匠，森山 英明
2．発表標題 プロセス間通信による機密情報拡散をKVMから防止する機能の検討
3．学会等名 電気・情報関係学会九州支部連合大会
4．発表年 2020年

1．発表者名 森山英明
2．発表標題 機密情報へのアクセスを解析する解析用VM作成手法の検討
3．学会等名 電気・情報関係学会九州支部連合大会（第72回連合大会）
4．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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

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