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　３ 年　 ６ 月　 ８ 日現在

機関番号：１５３０１
研究種目：若手研究
研究期間：2018～2020
課題番号：１８Ｋ１８０５１

研究課題名（和文）重要サービス保護のための仮想計算機モニタによる通信処理制御法の研究

研究課題名（英文）Research on Communication Controlling Method for Protection of Essential Services on Virtual Machine

研究代表者
佐藤　将也（Sato, Masaya）

岡山大学・自然科学研究科・助教

研究者番号：３０７５２４１４

交付決定額（研究期間全体）：（直接経費）　　2,500,000円

研究成果の概要（和文）：計算機の扱う情報の増加に伴い、計算機の扱う情報を狙った攻撃手法は複雑化し高度化している。攻撃の検知や防止を目的としたサービス（重要サービス）が攻撃の被害に遭うと、攻撃を防止できず被害が拡大する可能性がある。そこで、重要サービスの特定を困難化することで、重要サービスへの攻撃を回避する手法を提案した。具体的には、仮想計算機において、通信処理をもとにした重要サービスの特定を回避するために、通信処理を代理実行させる手法を提案し実現した。実験により、重要サービスによる通信内容の監視が困難にできることを確認した。また、性能評価により、提案手法による性能低下を抑制できていることを示した。

研究成果の学術的意義や社会的意義
本研究は、計算機への攻撃を直接的に防止するものではなく、事前に攻撃が困難な環境を構築するための研究である。また、近年普及しているクラウドの基盤となる仮想計算機技術を応用した研究である。さらに提案手法は、仮想計算機基盤の改変のみにより実現しており、既存のセキュリティ機構と併用が可能な構造を実現している。以上のことから、本研究の成果は、近年増加しつつあるサイバー攻撃への対策として有効なだけでなく、社会的に広く普及しつつある計算機環境におけるセキュリティを向上するための基礎技術の一つとして意義のあるものである。

研究成果の概要（英文）：Computers are widely used and also become a target of attacks aiming acquisition of information on the computer. Protection for essential services such as security software logging programs (we call these services essential services) is important. To avoid attacks on essential services, we proposed a method to make the behavior of the essential services invisible to attackers. The method monitors the behavior of the essential services on a virtual machine and transfers the processing to another virtual machine. With the proposed method, attacks on the virtual machine cannot monitor the communication of the essential service so finding the attack target becomes difficult.

研究分野：情報セキュリティ

キーワード：情報セキュリティ　マルウェア対策　仮想化技術

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

計算機の扱う情報の種類や量は年々拡大し、それに伴い計算機の扱う情報を狙った攻撃手法は複雑化し高度化している。これまでに攻撃の検知や防止を目的として様々な手法が研究開発されている。これらの手法は計算機を対象としたものとネットワークを対象としたものに分けられる。本研究では、計算機を対象とした保護手法を対象とする。計算機を対象として、攻撃による被害を防止する研究の中でも、攻撃を検知するものや攻撃を防止する手法が研究されている。これらの多くは、攻撃の手法に着目している。しかし、攻撃者の行動に着目した研究は多くない。また、攻撃を防止する手法を開発したとしても、それを実現するソフトウェアの動作を妨害された場合、攻撃を防止できない。そこで、セキュリティソフトウェアのように、攻撃の被害を抑制する為のサービス（以降、重要サービス）を攻撃者から不可視化することで、重要サービスへの攻撃を回避する手法を研究が重要である。また、この手法を実現するために、仮想計算機モニタ（Virtual Machine Monitor、以降、VMM）を用いる。仮想計算機モニタは、クラウドサービスなどの基盤ソフトウェアとして利用されており、仮想計算機（Virtual Machine、以降、VM）上で動作するソフトウェアから隔離されており安全性が高い。そこで、既存のセキュリティ機能を VMM に移植する手法が研究開発されている。しかし、VMM を用いたセキュリティ技術の多くは、既存の応用プログラムやオペレーティングシステムのカーネル機能一部として実現されており、これらの機能を VMM に移植する工数は小さくない。そこで、本研究では、既存の重要サービスを VMM に移植するのではなく、既存のソフトウェアを改変することなく、重要サービスを VMM により不可視化することで、攻撃を回避する手法の研究を行う。

２．研究の目的

本研究の目的は、重要サービスを提供するプロセス（以降、重要プロセス）からの通信内容を攻撃者から不可視化することで、通信内容を元にした重要サービスの特定を回避することである。具体的には、重要プロセスによる通信を代理実行する VM と代理プロセスを用意し、重要プロセスからの通信を代理プロセスにより実行する。この際、重要サービス自体は通信を行わないことにより、重要プロセスと同じ VM で動作する他のプログラムからは、重要プロセスの通信先や通信内容の特定を困難にする。また、背景で述べたとおり、重要サービスへの改変なしに機構を実現することで、多くの重要サービスを改変なしに保護可能な機構の実現を目的とする。

３．研究の方法

本研究の全体像を図１に示す。本研究における提案機構では、VMM を用いることで、重要サービスが動作する VM（保護対象 VM）上の重要プロセスによる通信を検知し、通信に関する情報を代理プロセスが動作する VM（代理 VM）に転送する。代理プロセスは、受け取った情報をもとに通信処理を代理実行し、通信結果を重要プロセスに返却する。本研究では以上の手法により、保護対象 VM 上の重要プロセス以外のプロセス（通常プロセス）とカーネルレベルの悪意あるソフトウェア（マルウェア）による重要サービスの特定を困難化する。

本研究は、重要プロセスに関する情報を不可視化することで、攻撃を先回りして攻撃対象の特定すら困難化することで攻撃を回避する。これは、個々の攻撃に対処する既存技術とは異なる。既存研究の多くは、応用プログラムの利用するメモリやファイルの不正な改変など、個々の攻撃への対処を提案しているものが多い。一方で、本研究は、攻撃対象の応用プログラムの特定すら困難にすることで、重要サービスが攻撃を受ける可能性を低減する。また、既存の重要サービスの改変なしに提案手法を実現することで、既存研究による成果を活かしつつ、本研究により既存の重要サービスへの攻撃を回

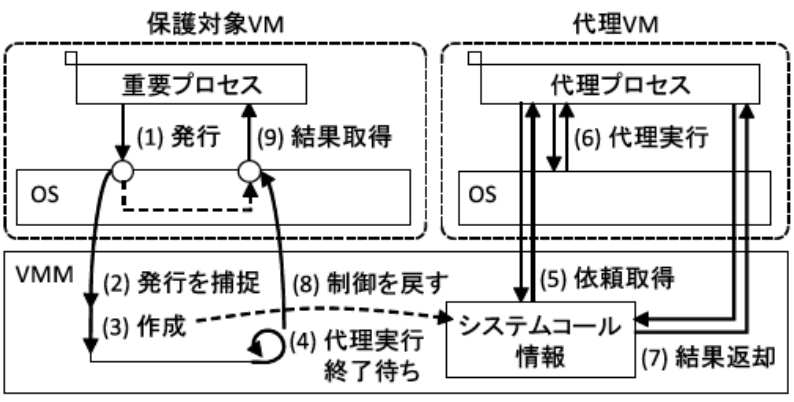

図１　重要サービスによる通信処理の不可視化手法

避するという多重の防御により、攻撃がより困難な環境を構築する。

本研究では、以下の項目に対処する。(1)重要プロセスの通信に関する情報の不可視化、(2)提案手法の性能評価と実在する攻撃を用いた有効性評価、(3)重要プロセス数と VM 数による性能への影響の明確化。(1)について、具体的には、通信内容の取得方法、代理プロセスへの転送方法、代理実行の方法、及び代理実行結果の返送方法を設計し、実現する。(2)ついて、(1)で実現した機構を用いて、実用される応用プログラムを利用した性能評価を行う。また、通信内容を監視する攻撃を実行し、攻撃への耐性を評価する。(3)について、重要サービスの数、保護対象 VM の数、および代理実行プロセスの数等の観点から、重要プロセスの性能を評価する。また、重要プロセスだけでなく、通常プロセスの性能へ与える影響も評価する。

４．研究成果

保護対象 VM 上の重要プロセスについて、通信処理を VMM により検知し、通信内容を保護対象 VM から代理 VM に転送する手法を実現した。また、代理 VM 上の代理プロセスが通信処理を実行し、実行結果を重要プロセスに返送する手法を実現した。提案手法は、保護対象 VM 上で Linux が動作し、VMM として Xen を用いる環境で実現した。提案手法では、重要プロセスによる通信処理の検知、通信内容の代理 VM への転送、代理実行結果の返送において、重要プロセスのプログラムを改変することなく、VMM により保護対象 VM のメモリとレジスタを操作することで実現した。これにより、保護対象 VM 上の既存ソフトウェアの改変なしに重要プロセスの通信処理を代理実行する方法を実現した。

提案手法の有効性を評価するために、保護対象 VM 上の通常プロセスから重要プロセスの通信処理の監視を試行し、提案手法により通信処理が不可視化されていることを確認した。具体的には、strace や tcpdump など、システムコールやパケット観測による通信処理の監視を行なった際に、提案手法が未適用の環境では観測できる情報が提案手法により観測を防止できていることを確認した。

性能評価では、詳細な性能分析として、通信処理の検知、代理実行の依頼処理、代理実行処理、および実行結果の返送処理に要する処理時間を明らかにした。また、応用プログラムの性能への影響を、重要プロセスによる通信処理性能、通常プロセスの処理性能、および Web サーバを用いたスループットの測定により明らかにした。詳細な性能分析の結果から、(1)通信処理の検知から実行結果の返送までに要する処理の期間中に保護対象 VM に CPU が割り当てられないことにより、通常プロセスの処理性能がお大きく低下することが明らかになった。また、(2)重要プロセスによる通信処理が発生したか否かの有無を代理プロセスが周期的に観測することにより、通信処理性能が最大で観測周期（1ms）だけ遅延し、通信処理性能への影響が大きいことを明らかにした。

以上の性能評価の結果をもとに、提案手法における性能低下の改善手法を提案し、実現した。1 つ目の問題への対処として、代理実行する間における保護対象 VM の停止回避を実現した。図 2 に、保護対象 VM の停止回避の処理の流れを示す。具体的には、重要サービスによる通信処理を VMM が検知した後、重要プロセスにすぐに処理を返却し、重要サービス以外のプロセスに CPU 使用権を譲るシステムコールを発行させることで対処した。これは、VMM が保護対象 VM のプログラムカウンタを当該システムコールを指すように改変した後に保護対象 VM に処理を返却することで実現した。また、当該システムコール終了時に、代理実行処理が終了したか否かを監視し、代理実行処理が終了していない場合には再度 CPU 使用権を譲らせ、代理実行処理が終了している場合は結果を重要プロセスに返却して処理を継続させることで、代理実行処理を可能にしつつ、通常プロセスにも CPU を割り当てることにより、通常プロセスの性能低下の問題へ対処した。保護対象 VM の停止回避による効果を明らかにするために、通常プロセスの処理性能を測定した結果を図 3 に示す。図 3 の評価結果より、通常プロセス（図中の他プロセス）について、VM 停止回避を適用した場合にスループット低下を抑制できていることを示した。

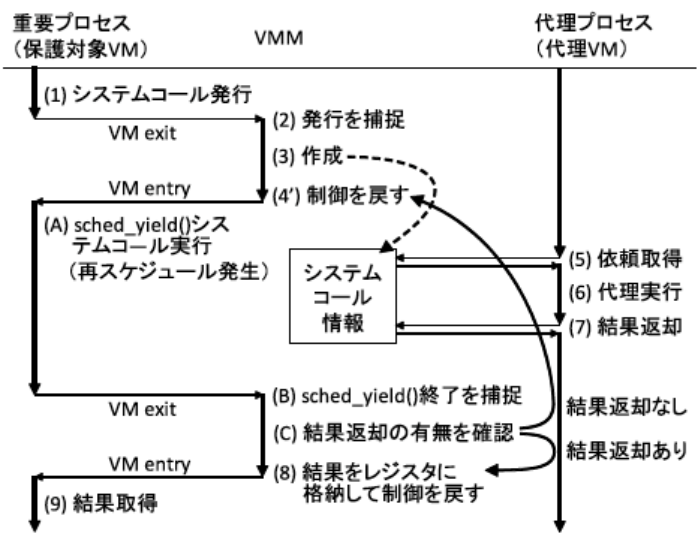

図２ CPU 使用権の移譲を用いた保護対象 VM の停止回避

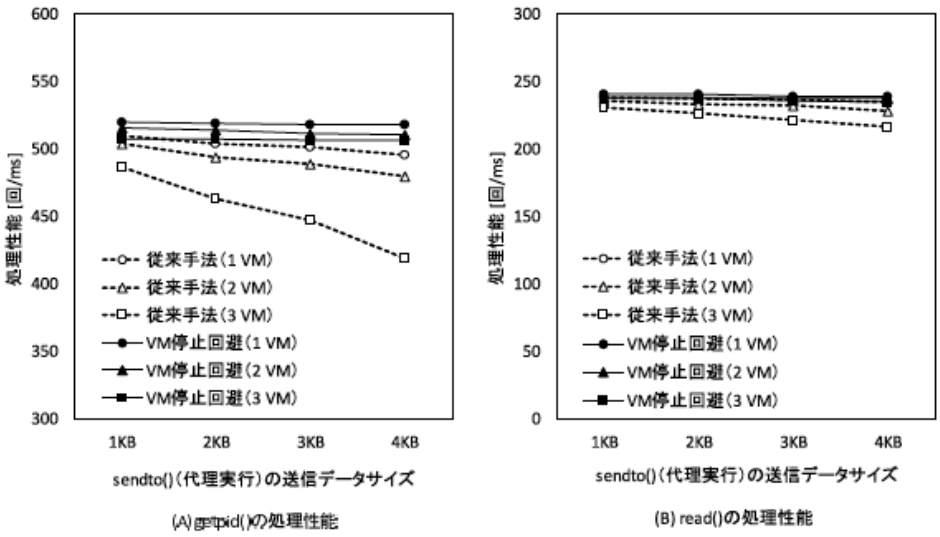

図 3 他プロセスが発行するシステムコールの処理性能

また、2 つ目の問題への対処として、代理実行の有無を VMM の持つイベント通知機構を用いた。図 4 にイベント通知機構を用いた依頼取得の処理の流れを示す。これにより、代理プロセスが代理実行の有無を監視する必要がなくなり、観測周期分の遅延発生を抑制する機構を実現した。イベント通知機構を用いた依頼取得による改善結果を図 5 に示す。依頼取得において発生するオーバヘッドについて、システムコールごとに依頼発生から依頼取得までの処理時間をオーバヘッドとして測定した。図 5 の結果より、イベント通知機構を用いることで、依頼取得処理におけるオーバヘッドが大幅に改善していることを示した。

以上より、重要サービスによる通信処理の不可視化機構の実現方式を示した。提案手法により、通信処理を観測することによる重要サービス特定を困難化できていることを示した。また性能評価により、性能低下の主要因となる 2 つの処理を明らかにして、性能低下の改善策を提案した。

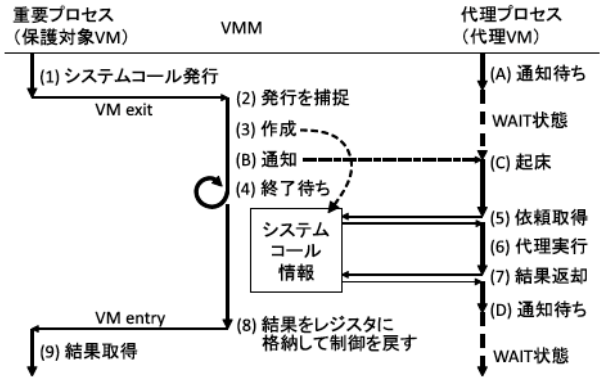

図 4 イベント通知機構を用いた依頼取得

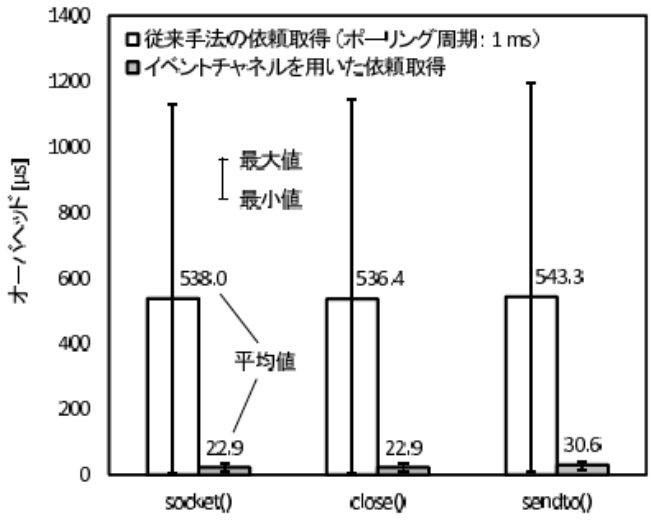

図 5 依頼取得におけるシステムコールオーバヘッド

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4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 奥田勇喜，佐藤将也，谷口秀夫	４．巻 61
２．論文標題 重要サービスの動作不可視化手法におけるシステムコール代理実行処理の効率化	５．発行年 2020年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1495-1506
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 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 Masaya Sato、Hideo Taniguchi、Toshihiro Yamauchi	４．巻 9
２．論文標題 Design and implementation of hiding method for file manipulation of essential services by system call proxy using virtual machine monitor	５．発行年 2019年
３．雑誌名 International Journal of Space-Based and Situated Computing	６．最初と最後の頁 1-10
掲載論文のDOI（デジタルオブジェクト識別子） 10.1504/IJSSC.2019.100007	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 Yuuki Okuda、Masaya Sato、Hideo Taniguchi	４．巻 9
２．論文標題 Implementation and Evaluation of Communication-Hiding Method by System Call Proxy	５．発行年 2019年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 217-238
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 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 Masaya Sato, Hideo Taniguchi, Toshihiro Yamauchi	４．巻 印刷中
２．論文標題 Design and Implementation of Hiding Method for File Manipulation of Essential Services by System Call Proxy using Virtual Machine Monitor	５．発行年 2019年
３．雑誌名 International Journal of Space-Based and Situated Computing	６．最初と最後の頁 印刷中
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 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10件（うち招待講演　0件／うち国際学会　3件）

１．発表者名
Masaya Sato, Hideo Taniguchi, Ryosuke Nakamura

２．発表標題
Virtual Machine Monitor-based Hiding Method for Access to Debug Registers

３．学会等名
The Eighth International Symposium on Computing and Networking（国際学会）

４．発表年
2020年

１．発表者名
佐藤将也、谷口秀夫、仲村亮祐

２．発表標題
VMMによるデバッグレジスタの読み出しと書き込みの隠蔽手法の提案

３．学会等名
情報処理学会第184回マルチメディア通信と分散処理研究会

４．発表年
2020年

１．発表者名
佐藤将也，谷口秀夫，鵜島匠

２．発表標題
様々な仮想計算機におけるディスク入出力性能の比較

３．学会等名
第148回システムソフトウェアとオペレーティング・システム研究会

４．発表年
2020年

１．発表者名
奥田勇喜，佐藤将也，谷口秀夫

２．発表標題
重要サービスの動作不可視化における仮想計算機停止の回避

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
奥田勇喜，佐藤将也，谷口秀夫

２．発表標題
システムコールの代理実行における仮想計算機停止時間の削減

３．学会等名
第18回情報科学技術フォーラム（FIT2019）

４．発表年
2019年

１．発表者名
佐藤将也，谷口秀夫，鵜島匠

２．発表標題
仮想計算機におけるディスク入出力性能の比較

３．学会等名
第18回情報科学技術フォーラム（FIT2019）

４．発表年
2019年

１．発表者名
奥田勇喜，佐藤将也，谷口秀夫

２．発表標題
VMMを用いて重要サービスの通信操作を不可視化する通信処理制御法

３．学会等名
情報処理学会第143回システムソフトウェアとオペレーティング・システム研究発表会

４．発表年
2018年

１．発表者名
Masaya Sato, Hideo Taniguchi, Toshihiro Yamauchi

２．発表標題
Hiding File Manipulation of Essential Services by System Call Proxy

３．学会等名
The 7-th International Workshop on Advances in Data Engineering and Mobile Computing (DEMoC-2018)（国際学会）

４．発表年
2018年

１．発表者名 佐藤将也，谷口秀夫，山内利宏
２．発表標題 仮想計算機を用いた重要ファイル保護手法の評価
３．学会等名 情報処理学会第17回情報科学技術フォーラム（FIT2018）
４．発表年 2018年

１．発表者名 Yuuki Okuda, Masaya Sato, Hideo Taniguchi
２．発表標題 Hiding Communication of Essential Services by System Call Proxy
３．学会等名 The Sixth International Symposium on Computing and Networking (CANDAR'18)（国際学会）
４．発表年 2018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