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　元 年　 ６ 月　 ５ 日現在

機関番号：１５３０１
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０２８２９

研究課題名（和文）仮想化環境と制御システムの証拠保全を実現する基盤ソフトウェアの研究

研究課題名（英文）Research for fundamental software of evidence preservation for virtualization environment and control system

研究代表者
山内　利宏（Yamauchi, Toshihiro）

岡山大学・自然科学研究科・准教授

研究者番号：８０３５９９４２

交付決定額（研究期間全体）：（直接経費）　　11,100,000円

研究成果の概要（和文）：計算機上で複数のゲストOSを動作させることができる仮想計算機環境で，複数のゲストOS内の機密情報の拡散を同時に追跡するためのゲストOSの識別手法とオーバヘッド削減手法について設計し，基本方式を実現した．また，ファイルシステムに痕跡を残さないマルウェアを解析するために，低オーバヘッドで，メモリ上のデータを保全する基本方式を実現した．

研究成果の学術的意義や社会的意義
仮想化環境での仮想マシン利用が普及しており，仮想マシン内の機密情報の拡散や利用状況の把握は重要である．本研究では，同じ仮想マシンモニタ上で動作する複数の仮想マシン内の機密情報を同時に追跡する基本方式を実現した．また，悪意のあるソフトウェアであるマルウェアが高度化し，ファイルシステムに痕跡を残さず，メモリ上にだけ存在するマルウェアが問題となっている．このようなマルウェアを解析する基本方式を提案した．

研究成果の概要（英文）：In a virtual machine environment where multiple guest OSs can run, we designed a guest OS identification method and overhead reduction method for simultaneously tracing the diffusion of classified information in each guest OS.In addition, in order to analyze malware that leaves no trace information in the file system, we proposed a basic method to preserve data in memory with low overhead.

研究分野：システムソフトウェア

キーワード：情報セキュリティ　デジタルフォレンジックス　マルウェア対策　OS　仮想化技術

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

サイバー攻撃の手口は年々高度化し，社会において大きな脅威となっている．特に，標的型攻撃は，攻撃対象を狙って行われる攻撃であり，発見が難しく，被害を受けたときの損害が大きくなる傾向がある．このため，サイバー攻撃に対抗する技術の研究開発が不可欠である．

サイバー攻撃の対象としては，政府機関や民間企業などが持つ重要な情報がある．当然，これらの組織では，必要なセキュリティ対策は最低限取られているものの，利用者がマルウェアの仕込まれたプログラムを誤って実行してしまう人為的ミスまで完全に防ぐことは難しい．また，最新のセキュリティパッチを適用していたとしても，未知の脆弱性を用いたゼロデイ攻撃が実際に使用されており，攻撃を完全に防ぐことができないという前提で対策を講じる必要がある．このために，攻撃を発見したときに，攻撃者の行動を把握し，被害の範囲を正確に特定でき，かつ電子的な証拠としても保存できる技術の確立が望まれている．

一方で，攻撃対象として，重要インフラの基幹システム（制御システム）を狙う攻撃の危険性が指摘されている．近年，制御システムは，汎用 OS や TCP/IP などの標準プロトコルを採用しつつあり，かつインターネットに接続されるものもあり，サイバー攻撃へのリスクが指摘されている．通常の情報システムとは違い，制御システムは，機密性や完全性よりも，可用性が重視される．これは，重要なインフラを制御している場合，制御システムが止まってしまうと，人命や生活に直接影響が出てしまうため，24 時間動かし続ける必要があるためである．このため，制御システムでは，可用性を確保したまま，サイバー攻撃への対策と証拠保全が求められる．

２．研究の目的

現在，非常に多くのサイバー攻撃が行われており，サイバー攻撃に対抗する技術の研究開発が急務である．また，サイバー攻撃により，侵入されることは完全には防げないため，侵入を前提として，被害を把握し，被害を抑制し，かつ被害の証跡を残すことが重要である．本研究では，今後ますます重要度が増すと考えられる仮想化環境と制御システムを対象として，サイバー攻撃に対抗するために，証拠保全を行うデジタルフォレンジック技術に着目し，被害範囲の把握や証拠保全を行う新しい技術の研究開発を行う．特に，仮想マシン環境を想定した侵入検知と防止技術と証拠保全技術，および 24 時間運転しなければならない制御システムを対象としたライブフォレンジック技術について，システムソフトウェアの観点からより安全なシステムの実現を目指す．

３．研究の方法

本研究では，上記 2 つの課題に対応するために，次の 2 つの研究を行う．

（研究１）サイバー攻撃による攻撃者の行動の把握，被害の把握，および電子的な証拠保全を実施可能にする仮想化技術の研究開発

（研究２）制御システムの可用性を損なわないライブフォレンジック技術の研究開発

（研究１）について，サイバー攻撃の手口の高度化により，オペレーティングシステム(OS)レベルのセキュリティ対策だけで防ぐことができる攻撃には限りがあり，OS よりも低レイヤーで動作し，攻撃されにくい仮想マシンモニタレベルでのセキュリティ対策が今後必要になると考えている．

また，仮想化技術は，特にクラウドコンピューティングでよく用いられている．仮想化技術によるセキュリティ機構を実現するに当たり，多数のゲスト OS に対してセキュリティ機能を適用できる方式を確立する必要がある．

上記の要求に対応するため，これまでに研究代表者らが研究開発してきた仮想化技術をベースとしたセキュリティ機構を元に，新たなセキュリティ機構の研究開発を行う．国内外では，ゲスト OS の状態を仮想マシンモニタから観測する研究が行われているものの，機密情報の伝搬に着目した研究は少ない．仮想化技術と Taint 解析を組み合わせた方法があるものの，システムコールレベルで追跡する本研究に比べ，追跡の粒度が必要以上に細かいことにより性能低下が大きく，実用上は問題が多いため，本研究では，システムコールレベルで追跡する手法を元に，研究を進める．

これまで単一のゲスト OS のみを対象としていた仮想マシン内部の機密情報の流れを追跡する手法を，同時に複数の仮想マシンを対象に追跡できるように拡張する．また，機密情報の流れを追跡するために取得する情報の種類や取得箇所の増減により，仮想化基盤ソフトウェアのセキュリティ機構が仮想マシンの性能に与える影響を明らかにする．

また，監視対象の仮想マシンの台数に対して，どのようにオーバヘッドが増加するのかを明らかにし，低オーバヘッドで情報取得可能なセキュリティ機構を実現する．

（研究２）について，サイバー攻撃の対象に，社会に影響を与える制御システムが含まれており，制御システムの安全性向上が望まれている．制御システムでは，可用性が重要であるため，セキュリティインシデントが起こった際に，制御システムのサービスを止めることなく，動作中のプロセスの解析や，解析対象のデータを取得し，保全する必要がある．

これまでの OS の研究の知見を生かし，制御システムのサービスを継続したまま対象プロセスのメモリイメージやディスクイメージを解析対象計算機に保存し，外部計算機に転送する課題

を解決する．
制御システムの実行プロセスの状態を低オーバヘッドで複製し，制御システムの可用性を低下させずに，メモリ上のプロセス状態が更新されて失われないように保全し，メモリ上で解析する手法を確立する（メモリフォレンジック）．制御システムの可用性を維持したまま，メモリ上のプロセスのデータを解析する技術を実現する．

４．研究成果

（研究１）についての成果

・複数の仮想マシン上の機密情報の拡散追跡機能についての実現

従来は，同時に１つの仮想マシンのみの機密情報の追跡が可能であった．そこで，複数の仮想マシンを同時に追跡する課題について明確化した．

一つ目の課題として，仮想マシンのシステムコール発行した際に，どの仮想マシン内のシステムコール発行なのかを把握する必要がある．仮想マシンの識別のためには，仮想マシンに固有のユニークな ID を識別に用いる方法は参照のオーバヘッドが大きいことを明らかにし，仮想マシンの実行開始時に決まる動的な情報を併用することで，そのオーバヘッドを削減できることを明らかにした．具体的には，UUID と構造体のアドレスを併用する方式を提案し，複数の仮想マシンのシステムコール発行を識別できることを示した．また，拡散している機密情報を格納する管理表を，複数の仮想マシンの追跡のために拡張する必要がある．拡張した管理表を設計し，仮想マシン毎に追跡できることを示した．

同時に複数の仮想マシンを対象に追跡する手法の性能上の課題を詳細に分析し，性能オーバヘッドの詳細な分析を行った．具体的には，同時に多数の VM を走行させた場合のオーバヘッド，及びファイルアクセス処理を行ったときのオーバヘッドを詳細に分析した．

・単体の仮想マシンの機密情報の追跡におけるオーバヘッド要因の特定と改善

VMM から仮想マシン上の情報を取得するには，セマンティックギャップがあり，情報の取得や取得した情報の解釈が難しい．このため，システムコールを契機として，機密情報の追跡処理におけるオーバヘッドが問題となっている．この問題に対処するため，単体の仮想マシンの機密情報の拡散を追跡したときのオーバヘッドを評価し，オーバヘッドの大きい処理を明らかにした．

次に，オーバヘッドが大きい処理へのオーバヘッドの削減方法を検討した．削減法としては，ログの出力タイミングに着目した手法を提案し，その効果を予測した．また，ファイルパス取得処理のオーバヘッドも大きいため，機密情報の拡散追跡機能の処理においてファイルパス取得処理を削減したときのオーバヘッド削減の効果を予測した．

（研究２）についての成果

・シングルプロセッサを対象としたライブフォレンジック手法

シングルプロセッサを対象として，プロセスを複製してプロセスからメモリイメージのスナップショットを取得する方法を設計し，実現した．これにより，ファイルシステムに痕跡を残さない攻撃に対処できる．

・マルチコアプロセッサを対象としたライブフォレンジック手法

マルチコアプロセッサ環境において，メモリ上のプロセスの情報を保全する方式を提案し，その実現方式を示した．具体的には，従来はメモリ上の証拠保全を要求したプロセスのコンテキスト内で行っていた証拠保全処理を，証拠保全されるプロセスのコンテキスト内で行うように方式を再提案した．これにより，証拠保全をされるプロセスがマルチコア環境で動作する場合でも，メモリ上のデータの一貫性が取れた状態で証拠保全できることが期待できる．また，実装と評価により，提案方式を用いることで，実時間処理を行うプロセスに対しても，可能性を損なわずに証拠保全ができることを示した．

５．主な発表論文等

〔雑誌論文〕（計　６件）

① Masaya Sato, Hideo Taniguchi, Toshihiro Yamauchi, Design and Implementation of Hiding Method for File Manipulation of Essential Services by System Call Proxy using Virtual Machine Monitor, International Journal of Space-Based and Situated Computing, 査読有, vol.9, no.1, pp.1-10 (2019.05).

② 山内利宏，時松勇介，谷口秀夫，可用性を考慮したプロセスの複製によるライブフォレンジック手法，情報処理学会論文誌，査読有，vol.60，no.2，pp.696-705 (2019.02).

③ Yuuki Okuda, Masaya Sato, Hideo Taniguchi, Hiding Communication of Essential Services by System Call Proxy, 2018 Sixth International Symposium on Computing and Networking (CANDAR), 査読有, pp.47-56 (2018.11). DOI: 10.1109/CANDAR.2018.00014

④ Masaya Sato, Hideo Taniguchi, Toshihiro Yamauchi, Hiding File Manipulation of Essential Services by System Call Proxy, Lecture Notes on Data Engineering and

Communications Technologies, 査読有, vol.22, pp.853-863 (2018.09).

⑤ Hideaki Moriyama, Toshihiro Yamauchi, Masaya Sato, Hideo Taniguchi, Performance Improvement and Evaluation of Function for Tracing Diffusion of Classified Information on KVM, 4th International Workshop on Information and Communication Security (WICS 2017), Proceedings of 2017 5th International Symposium on Computing and Networking (CANDAR 2017), 査読有, pp.463-468 (2017.11). DOI: 10.1109/CANDAR.2017.91

⑥ Masaya Sato, Toshihiro Yamauchi, Hideo Taniguchi, Memory Access Monitoring and Disguising of Process Information to Avoid Attacks to Essential Services , Proceedings of 2016 Fourth International Symposium on Computing and Networking, 査読有, pp.635-641 (2016.11). 3rd International Workshop on Information and Communication Security DOI: 10.1109/CANDAR.2016.89

〔学会発表〕(計１６件)

① 森山英明, 山内 利宏, 佐藤将也, 谷口秀夫, 機密情報の拡散追跡機能におけるタイムリーな管理対象把握法, 情報処理学会第 81 回全国大会講演論文集, vol.第 1 分冊, pp.25-26 (2019.03).

② 荒木 涼, 森山英明, 山内 利宏, KVM を利用した機密情報の拡散追跡機能におけるファイルパス取得処理削減の評価, 情報処理学会第 81 回全国大会講演論文集, vol.第 3 分冊, pp.433-434 (2019.03).

③ 本田 匠, 森山英明, 山内 利宏, KVM における機密情報の拡散追跡機能を支援する可視化機構の検討, 情報処理学会第 81 回全国大会講演論文集, vol.第 3 分冊, pp.431-432 (2019.03).

④ 岡崎 俊樹, 森山英明, 山内 利宏, 佐藤将也, 谷口秀夫, KVM における機密情報の拡散追跡機能を用いた複数 VM 監視手法の評価, 情報処理学会第 81 回全国大会講演論文集, vol.第 3 分冊, pp.429-430 (2019.03).

⑤ 福本 淳文, 山内 利宏, KVM 上のゲスト OS における権限の変更に着目した権限昇格攻撃防止手法の実現, 情報処理学会研究報告, vol.2019-CSEC-84, no.7, pp.1-8 (2019.03).

⑥ 佐藤将也, 谷口秀夫, 山内 利宏, 仮想計算機を用いた重要ファイル保護手法の評価, 第 17 回情報科学技術フォーラム（FIT2018）講演論文集, vol.第 4 分冊, pp.171-172 (2018.09).

⑦ 森山英明, 山内 利宏, 佐藤将也, 谷口秀夫, KVM を利用した機密情報の拡散追跡機能におけるファイルアクセス性能の評価, 第 17 回情報科学技術フォーラム（FIT2018）講演論文集, vol.第 1 分冊, pp.147-148 (2018.09).

⑧ 奥田 勇喜, 佐藤将也, 谷口秀夫, 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, 情報処理学会研究報告, vol.2018-OS-143, no.2, pp.1-8 (2018.05).

⑨ 森山英明, 山内利宏, 佐藤将也, 谷口秀夫, KVM を利用した機密情報の拡散追跡機能における高速化の評価, 情報処理学会第 80 回全国大会講演論文集第 1 分冊, pp.1-2 (2018.03).

⑩ 時松 勇介, 山内 利宏, 谷口秀夫, プロセスの複製による可用性を考慮したライブフォレンジック手法のマルチコア対応と評価, コンピュータセキュリティシンポジウム 2017 (CSS2017) 論文集, vol.2017, no.2, pp.237-244 (2017.10).

⑪ 岡崎 俊樹, 森山英明, 山内 利宏, 佐藤将也, 谷口秀夫, KVM 上の複数 VM の動作に対応した機密情報の拡散追跡機能, コンピュータセキュリティシンポジウム 2017 (CSS2017) 論文集, vol.2017, no.2, pp.1295-1301 (2017.10).

⑫ 佐藤将也, 山内 利宏, 谷口秀夫, 仮想計算機を用いた重要ファイル保護手法, コンピュータセキュリティシンポジウム 2017 (CSS2017) 論文集, vol.2017, no.2, pp.1302-1308 (2017.10).

⑬ 森山英明, 山内利宏, 佐藤将也, 谷口秀夫, KVM における機密情報の拡散追跡機能の高速化, 第 16 回情報科学技術フォーラム(FIT2017)講演論文集, vol.第 1 分冊, pp.191-192 (2017.09).

⑭ 森山英明, 山内利宏, 佐藤将也, 谷口秀夫, KVM における機密情報の拡散追跡機能における性能改善策, 情報処理学会第 79 回全国大会講演論文集, vol.第 1 分冊, pp.13-14 (2017.03).

⑮ 時松 勇介, 山内 利宏, 制御システムの可用性を考慮したプロセスの複製によるライブフォレンジック手法の提案, コンピュータセキュリティシンポジウム 2016 (CSS2016) 論文集, vol.2016, no.2, pp.84-91 (2016.10).

⑯ 佐藤将也, 山内 利宏, 谷口秀夫, 攻撃回避のためのファイル不可視化手法の提案, コンピュータセキュリティシンポジウム 2016 (CSS2016) 論文集, vol.2016, no.2, pp.224-228 (2016.10).

〔図書〕(計　０件)

〔産業財産権〕
○出願状況（計　0件）

○取得状況（計　0件）

〔その他〕
ホームページ等
なし.

６．研究組織

(1)研究分担者

研究分担者氏名：谷口　秀夫
ローマ字氏名：Taniguchi Hideo
所属研究機関名：岡山大学
部局名：自然科学研究科
職名：教授
研究者番号（8 桁）：70253507

研究分担者氏名：森山　英明
ローマ字氏名：Moriyama Hideaki
所属研究機関名：有明工業高等専門学校
部局名：創造工学科
職名：講師
研究者番号（8 桁）：00633009

研究分担者氏名：佐藤　将也
ローマ字氏名：Sato Masaya
所属研究機関名：岡山大学
部局名：自然科学研究科
職名：助教
研究者番号（8 桁）：30752414