論文の内容の要旨及び論文審査の結果の要旨の公表

学位規則第 8 条に基づき、論文の内容の要旨及び論文審査の結果の要旨を公表する。

○氏名	大月　勇人（おおつき　ゆうと）
○学位の種類	博士（工学）
○授与番号	甲　第 1097 号
○授与年月日	2016 年 3 月 31 日
○学位授与の要件	本学学位規程第 18 条第 1 項 学位規則第 4 条第 1 項
○学位論文の題名	仮想化技術に基づいたマルウェア解析のためのシステムコールトレース手法に関する研究
○審査委員	（主査）毛利　公一　（立命館大学情報理工学部教授） 大久保　英嗣（立命館大学情報理工学部教授） 上原　哲太郎（立命館大学情報理工学部教授）

＜論文の内容の要旨＞

本論文は、悪意あるソフトウェア（マルウェア）がソフトウェアシステムの脅威となっている問題に対し、マルウェアを動作させてその挙動を観測する動的解析技術を新たに提案し、解決に寄与するものである。既存研究の課題とされる次の 3 点に着目している。

（1）マルウェア自身が動的解析対象となっていることを検出し、実行停止や解析妨害をするアンチデバッグ機能への対策。既存研究の動的解析システムはマルウェアから容易に検出されてしまう特徴を有している。

（2）動的解析にかかる時間の対策。既存研究の動的解析システムはオーバヘッドが大きく、短時間での解析ができない。

（3）マルウェアが正規プロセスのメモリ空間内にコードを挿入して実行させるプロセス感染型マルウェアへの対策。既存研究の動的解析システムの観測単位がプロセスであるため、正規プロセス内の正規の挙動と悪意ある挙動を区別できない。

これらに対し、軽量な仮想計算機モニタをベースとするシステムコールトレーサ Alkanet を提案し実現した。仮想化技術により、マルウェアから容易に検出できない仮想環境を構築し（1）を解決した。評価では典型的なアンチデバッグ手法の 94%に対して耐性があることを確認した。仮想化技術により、必要なタイミングでのみ挙動を観測することで（2）を解決した。評価では実機の 78%の性能で動作することを確認した。システムコール発行時の関数呼出し階層をプロセッサの分岐記録機能を用いて取得する機能を Alkanet 内に設け、かつゲスト OS のメモリ管理情報と発行されたシステムコールの情報を

用いて感染領域を識別する解析法を提案し（３）を解決した。

＜論文審査の結果の要旨＞

本論文の主要な研究成果は以下のようにまとめることができる。

１．Type1 の仮想計算機モニタ（VMM）内にゲスト OS 観測機構を構築した点

既存研究の動的解析システムの多くは、詳細情報を容易に取得すべく Type2（ホスト OS 上でエミュレータとして動作する形態）の VMM を用いている。そのため、実装が比較的容易であるが実行速度が遅く、アンチデバッグ機能に検出される。Alkanet は Type1（ハードウェア上で直接 VMM が動作し、その上でゲスト OS が動作する形態）の VMM を用いてゲスト OS 内部のデータ構造を取得するための緻密な機構が実装されている点が注目すべき特徴であり評価できる。その結果、次のようなメリットを実現した。

- システムコール発行時と終了時にのみ観測処理を実行し、それ以外は実機と同様の速度で実行できるため、オーバヘッドの大幅軽減に成功している。
- Alkanet のベースとした VMM は、ハードウェアエミュレーションを行っていないため、実機のデバイスをそのままゲスト OS に見せることができる。よって、マルウェアのアンチデバッグ機能の無効化に成功している。

２．信頼できる関数呼出し階層の構築手法と感染領域の識別法を実現・融合した点

従来、関数呼出し階層の取得にはプロセスのスタックをたどる手法が用いられていたが、この手法ではマルウェアが偽装可能である。本論文では、プロセッサの分岐記録情報を用いて関数呼出し階層を取得する手法を提案し、マルウェアによる偽装を不可能とした点に新規性がある。これにより、どのようなメモリ領域に置かれた関数を経由してシステムコールが発行されたのかについて、信頼できる情報の取得に成功している。

加えて、他プロセスのメモリ領域へのアクセス、メモリ領域の属性変更、スレッド生成などのシステムコールを関連づけて解析する手法が提案されている。これによって、感染型マルウェアであっても、正規のシステムコール呼び出しか、悪意があるものかを判断することに成功している。このような詳細な解析を行っている点が評価できる。

以上、実問題に対して有効な新たな手法を提案し、高度な実装によって解決している。さらに、適切な評価がなされており有効性が実証されている。

本論文の審査に関して、2016 年 2 月 4 日（木）10 時 00 分～11 時 00 分情報システム学科会議室において公聴会を開催し、学位申請者による論文要旨の説明の後、審査委員は学位申請者大月勇人氏に対する口頭試問を行った。各審査委員および公聴会参加者より、提案手法の限界、自動解析や手動解析との関連性、マルウェア対策全体への寄与と今後の発展性などについての質問がなされたが、いずれの質問に対しても学位申請者の回答は適切なものであった。よって、以上の論文審査と公聴会での口頭試問結果を踏まえ、本論文は博士の学位に値する論文であると判断した。

＜試験または学力確認の結果の要旨＞

本論文の主査は、学位申請者と本学大学院情報理工学研究科情報理工学専攻博士課程後期課程在学期間中に、研究指導を通じ、日常的に研究討論を行ってきた。また、本論文提出後、主査および副査はそれぞれの立場から論文の内容について評価を行った。

学位申請者は、本学学位規程第 18 条第 1 項該当者であり、在学期間中の研究活動、論文内容の評価および公聴会での質疑応答を通して、学位申請者が十分な学識を有し、博士学位に相応しい学力を有していると確認した。

以上の諸点を総合し、学位申請者に対し、本学学位規程第 18 条第 1 項に基づいて、「博士（工学　立命館大学)」の学位を授与することが適当であると判断する。