学位論文の審査結果の要旨

本学位論文は，文書型マルウェアのシェルコード特定と圧縮・暗号化されたマルウェアの復号手法，ならびに亜種の自動分類のためにAPIコールグラフのクラスタ解析を行う静的解析手法と試作ツールの性能評価について明らかにした内容である．マルウェアはコンピュータセキュリティにおける脅威の1つである．マルウェア対策を行うためには，マルウェアを解析してマルウェアの動作・機能を知る必要がある．申請者は，文書型マルウェアからシェルコードを抽出する方法，パックされたマルウェアを展開してオリジナルのコードを抽出する方法，大量のマルウェアを分類する方法を提案した．文書型マルウェアに対しては，Microsoft Officeの文書ファイルから文書ファイルを開くアプリケーションを用いずにシェルコードを特定する方法について検討した．文書ファイルのエントロピーに基づいて，シェルコードの候補となるバイト列をエミュレータで実行することで効率よくシェルコードを特定することを試みる．特定したシェルコードを動的解析するための実行可能ファイルを作成することで，文書ファイルを開くアプリケーションで脆弱性が攻撃されてシェルコードが実行された状態を再現できる．これにより，シェルコードによって作成される実行可能ファイルを得る．本論文では，実際の文書型マルウェアを用いて，シェルコードの特定を試みて成否を確認した．また特定したシェルコードを実行して動作を観測した．本論文では圧縮・暗号化された実行可能ファイルを復号する方法についても検討した．申請者の提案する方法では，独自に作成したエミュレータにより実行可能ファイルの復号コードを実行することで元のバイナリイメージを取得する．このエミュレータは完全にソフトウェアで動作するのでマルウェアが動作する環境を用意する必要がない．復号に合わせてエントリーポイントの特定とインポートテーブルの再構築を行う．エントリーポイントの特定は自身が書き換えたメモリの実行を検知する方法，および既知のエントリーポイントのコードと比較する方法を用いる．本論文では実際のマルウェアの中で圧縮・暗号化された検体に対して復号とエントリーポイントの特定，インポートテーブルの再構築を試みた．また既知のプログラムをパックして，復号が可能であるか調査した．大量にあるマルウェアを効率よく解析するために，本論文ではマルウェアを分類する新たな方法について提案した．提案する方法ではマルウェアの分類のために，逆アセンブルした結果を制御フロー解析し，あるAPIが呼び出された後に呼び出される可能性のあるAPIの対（API推移）を抽出する．API推移の推移を比較することで，マルウェア間の類似度を算出して階層型クラスタ解析を行う．実際のマルウェアを分類することでパフォーマンス

評価を行い，マルウェアのソースコードをコンパイラおよびコンパイラのオプションを変更してコンパイルしたバイナリから類似度を求めることで性能評価を行った．最後に本論文では，マルウェアの静的解析に対して本論文で提案する方法の有効性について議論し，今後の課題について述べている．

以上の内容を有する本学位論文は，申請者を筆頭著者とする審査付き原著論文２編と国際会議論文２編に基づいてまとめられており，当講座の学位審査の目安を満足している．申請学位論文は学術的新規性が高く，情報セキュリティに関する研究および大規模解析領域における工学的応用にも貢献すると判断される．従って，本論文は，博士（工学）の学位論文として十分価値あるものと審査委員全員一致で判断した．

公表主要論文名

論文発表（１）（レフェリー制のある学術雑誌）

- 岩本一樹, 和﨑克己 : 文書型マルウェアに対するエントロピーとエミュレーションを用いたシェルコード特定方法 ; 情報処理学会論文誌, Vol.56, No.3, 2015. (2014 年 12 月 1 日採択済み)
- 岩本一樹, 和﨑克己 : 静的解析により抽出された API 推移に基づくマルウェアの分類 ; 情報処理学会論文誌, Vol.54, No.3, pp.1199-1210, 2013.

論文発表（２）（レフェリー制のある国際会議議事録）

- Kazuki Iwamoto, Katsumi Wasaki : A Method for Shellcode Extraction from Malicious Document Files using Entropy and Emulation ; Proceedings of the 4th International Conference on Security Science and Technology (ICSST2015), 7pages, (2014 年 10 月 20 日採択済み).
- Kazuki Iwamoto, Katsumi Wasaki : Malware Classification based on Extracted API Sequences using Static Analysis ; Proceedings of the 8th Asian Internet Engineering Conference (AINTEC2012), ACM Conference Proceedings, pp.31-38, 2012.