シンボリック実行を活用したマルウェア解析妨害機能の特定に向けた検討

Specifying Anti-analysis Techniques in Malware By Using Symbolic Execution

窪　優司・法制倫理分科会・情報セキュリティ大学院大学

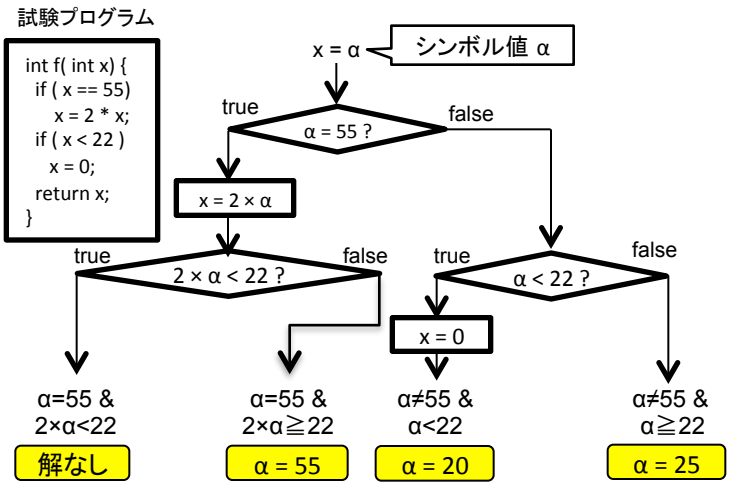
Understanding anti-analysis techniques embedded in malware binaries is crucial for malware analysis because recent malware often reveals the intended action after checking analysis environment. With symbolic execution, the constraints for hindering the analysis could be listed and revealed. The goal of this research is specifying the anti-analysis techniques and making malware reveal its intended action.

1. マルウェアの解析妨害機能

マルウェアはさまざまな解析妨害機能を保持し、自身の機能や意図を解析されないよう工作が施されている。

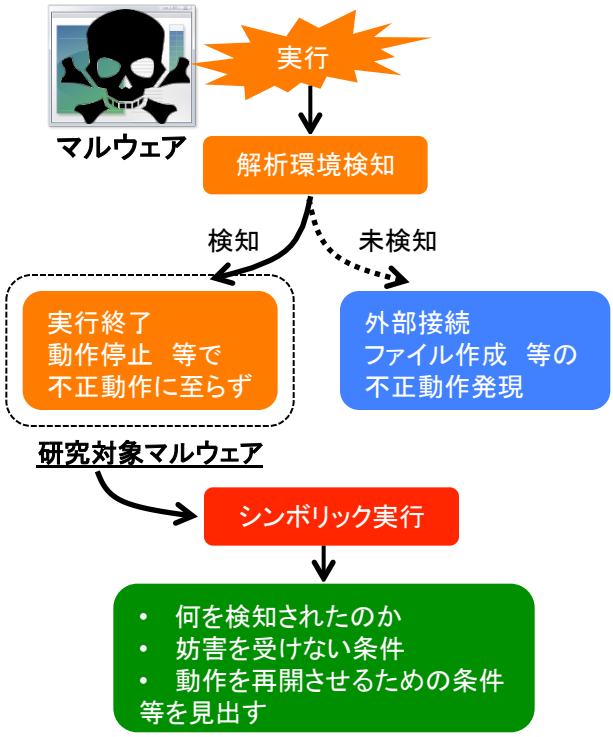
2. シンボリック実行

シンボリック実行は、プログラムが実行しうるパスを網羅的に抽出する技術であり、主にソフトウェア試験で活用されている。
プログラムに含まれる変数に具体値を入力せず、その代わりとして値を代表するシンボルの操作を通じてプログラムを模擬的に実行し，結果を評価する技術である。



3. シンボリック実行を活用した解析妨害機能の特定手法のイメージ

解析妨害機能を保持したマルウェアに対してシンボリック実行技術を適用し、当該機能の内容の特定と回避策の考案を目指す。



4. 今後の研究方針

- 既に複数存在しているシンボリック実行のためのフレームワークの機能比較およびマルウェア解析への適用可能性の調査
- プログラムを実行しつつシンボリック実行を適用する動的シンボリック実行技術についての調査
- 圧縮や暗号化が施されている実行ファイルに対してのシンボリック実行技術の適用可能性についてのさらなる調査・検討