5Z-6

Windows 上における危険な処理の承認機構の提案

早川　顕太†　　鈴木　秀和†　　旭　健作†　　渡邊　晃†

†名城大学理工学部

1　はじめに

マルウェアは多様化が進み，不正インストールやスパムメールの送信，情報漏えいといった様々な活動を行う．これらの活動はバックグラウンドで行われるためユーザがその危険な処理に気づくことができないという課題がある．

本稿では，Windows 上において危険な処理の承認機構を提案することにより，マルウェアがバックグランドで行う危険な処理を防止する．

2　既存技術

2.1　マルウェア検出の既存技術

マルウェア検出の手法はいくつかあるが，その中でも，未知・難読化マルウェアを検出可能な手法としてビヘイビア法が注目されている．ビヘイビア法は，事前にマルウェアの振る舞いを定義し，実際にマルウェアを動作させた上で，その振る舞いを検出する手法である．ビヘイビア法を用いて，ワームの自己複製やキーロギングを検出する研究[1,2]が存在する．しかしながら，ビヘイビア法には以下に示す課題がある．

- （課題 1）振る舞い定義の難しさ
  マルウェアは多様化が進み，様々な活動を行うため，マルウェアの振る舞いを一概に定義することができない．表 1 の左列に，マルウェアが行う可能性がある活動を示す．個々の活動を検出したとしても検出対象となるマルウェアの範囲は狭くなってしまう．
- （課題 2）正規ソフトウェアとの分離
  表 1 の右列に，マルウェアの活動に対して正規ソフトウェアが行う類似した活動を示す．マルウェアの活動の多くが正規ソフトウェアにも見られる活動であることが分かる．従って，これらの活動を検出対象としても誤検知の恐れがある．

課題 1 を解決する試みとして，振る舞い定義に機械学習を用いた研究[3]がある．しかし，課題 2 のために現状ではある程度の誤検知が生じてしまう．また，機械学習のため検出時にその理由をユーザに説明できないという課題がある．

提案方式は，Windows 上における危険な処理の承認機構である．ユーザの承認機構という方式を取ることで，インストールやメールの送信といった正規ソフトウェアにおいても観測される一部の活動を検出対象にできる．マルウェアと正規ソフトウェアの分離にはユーザの判断を借りることで，誤検知を少なくできる．

表 1．マルウェアと正規ソフトウェアの活動

マルウェアの活動	正規ソフトウェアによる類似活動
不正インストール	インストール
スパムメールの送信	メール送信
他プロセスの強制終了(セキュリティ無効化)	タスクマネージャ等による強制終了
掲示板への不正投稿	掲示板への正規投稿
キーロギング	キーバインド等
情報漏えい	データ送信
ファイル破棄・改ざん	ファイル削除・更新
バックドア	外部との通信
DDoS 攻撃	サーバへの通信
実行ファイルへの感染	アップデート
自己複製	なし
ルートキット	なし

2.2　承認機構の既存技術

現在，著者らの知る限り Windows 上において動的な承認機構を提供するといった研究はない．

承認機構に関連した既存技術としては，Windows Vista 以降に導入されたユーザアクセス制御（UAC;User Access Control）が挙げられる．UAC により，管理者のユーザとしてログインしても，昇格プロンプトによりユーザの承認を得ない限り，標準ユーザの権限として動作する．これにより，マルウェアがシステム全体に悪意のある変更を加えることを防止できる．

しかし，UAC はプログラムの起動時に行われる承認機構であり，プログラムの実行中に行われる動的な承認機構ではない．従って，昇格プロンプトを表示した時点では，実際に行われる処理の内容やそのタイミングをユーザが把握することができない．また，標準ユーザの権限で行える，カレントユーザのみへのシステムの変更

A Proposal of Approval Mechanisms for Dangerous Processing on Windows

†Kenta Hayakawa, Hidekazu Suzuki, Kensaku Asahi, and Akira Watanabe

Faculty of Science and Technology, Meijo University

や，メールの送信なども防ぐことができない．

3　提案方式

本稿では，Windows 上における危険な処理のユーザへの承認機構を提案する．具体的には，アプリケーションが危険な処理を行うために発行する Windows API を提案システムがフックすることで，その危険な処理が行われる直前に，ユーザへの承認ダイアログを表示する．ユーザは行われていようとしている危険な処理が自分の意図したものであるかどうかによって，その処理の許可／拒否を選択する．ユーザの応答により，提案システムはその処理を続行するか，あるいは処理を中断させアプリケーションにエラーを返す．これにより，マルウェアがバックグラウンドで行う危険な処理を，ユーザは自身の意図していないものとして拒否することができる（図 1）．

提案方式が承認機構として満たすべき 4 つの要件は以下の通りである．

【要件 1】検出対象となる処理はマルウェアによって行われる悪意のある活動であること．

マルウェアが行わない処理に承認を求めても意味がない．要件 1 を満たす処理として前述した表 1 のマルウェアの活動が挙げられる．

【要件 2】ユーザは処理を許可／拒否するための判断が可能であること．

承認ダイアログが表示され，その行われようとしている処理がユーザに身に覚えのないものならば，ユーザはそれを拒否できること（すなわち，そのプログラムがマルウェアであること）が求められる．このことが成り立つためには，検出対象となる処理が次の条件を満たしている必要がある．

「条件：任意の正規ソフトウェアは，ユーザが意図したタイミングのみにその処理を行う」

これは，つまり正規ソフトウェアがバックグラウンドで行う処理を検出対象の処理にすべきではないということを述べている．可能な限りこの条件を満たす処理を危険な処理として定義することで，提案方式はユーザによる誤検知を少なくできる．表 1 のマルウェアの活動に対する正規ソフトウェアの類似活動において，この条件を満たすものを危険な処理として表 2 のように定義する．

【要件 3】承認ダイアログ内に，ユーザの理解の助けとなるような付加的な情報を提示する．

この要件を満たすため，承認ダイアログ内には行われようとしている危険な処理の内容やその処理を行うプロセスに関する情報，また，そのプロセスが表示中のウインドウ等を表示する．

【要件 4】承認機構により，ユーザビリティが著しく損なわれないようにすること．

この要件を満たすため，提案方式はホワイトリストを導入する．プログラムを一定の期間使用し，ユーザがそれを安全であると判断した場合，そのプログラムの絶対パスと常に許可したい危険な処理（複数可）をホワイトリストへ登録する．それ以降，承認ダイアログは省略され，ユーザビリティは損なわれない．ただし，ホワイトリストに登録したプロセスにマルウェアがスレッドを注入することで，そのスレッドが許可された危険な処理を自由に行えてしまう．従って，ホワイトリストに登録されたプロセスに対してスレッドの注入や仮想メモリの書き込みなどを禁止することで，マルウェアから保護する必要がある．

表 2．危険な処理の定義

危険な処理	想定される被害
実行ファイルの作成	不正インストール
自動実行への登録	不正インストール
メールの送信	スパムメール
他プロセスの強制終了	セキュリティ無効化
HTTP の POST	掲示板への不正投稿
キー入力の取得	キーロギング

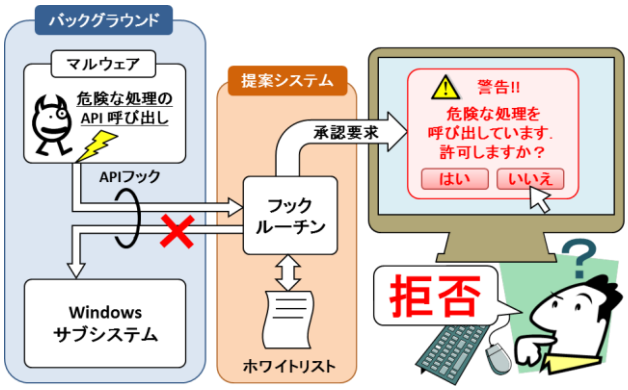

図 1．提案方式

4　むすび

本稿は，Windows 上でマルウェアがバックグラウンドで危険な処理を行うことを防止するため，ユーザへの承認機構を提案した．今後は，提案方式の実装と有用性の評価を行う予定である．

参考文献

[1]松本隆明ら，情報処理学会論文誌，Vol.48，No.9，3174-3182，Sep. 2007.
[2]松本隆明ら，情報処理学会論文誌，Vol.48，No.9，3137-3147，Sep. 2007.
[3]伊波靖ら，情報処理学会論文誌，Vol.50，No.9，2173-2181，Sep. 2009.