5W-03

検出対象動作とリスクを紐づけ対策行動へ誘導する警告手法

仁科 泉美† 大平 健司‡ 谷岡 広樹‡ 佐野 雅彦‡ 松浦 健二‡ 上田 哲史‡
徳島大学 工学部† 徳島大学 情報センター‡

1. はじめに

コンピュータを脅威から守るために，ユーザがセキュリティ警告に従うことは重要である．Windows 上では，ユーザアクセス制御（UAC; User Access Control）やアンチウイルスソフトウェアによる警告が該当する．しかし，コンピュータセキュリティに関する言葉を警告画面に用いているため，その知識が乏しいユーザは，警告内容を正しく理解できないという問題がある．早川ら[1]は，プログラム実行時に危険な処理を検知し，警告画面を表示する手法を提案している．警告画面は，防ぎたい処理を危険な処理として図や専門知識が乏しくても理解可能な用語で説明するが，その処理の問題点は示さない．つまり，ユーザはどのような事象が身に起こるかわからず，不適切に許可を選択する可能性があるため，提案された表示項目ではマルウェアの活動を防ぐには不十分であると考える．

そこで，本研究では Windows 上で実行されるソフトウェアについて，ユーザがソフトウェアの脅威を理解し行動選択するセキュリティ警告手法を提案する．

2. 提案手法

2.1 セキュリティ警告表示の要件

本手法では，ソフトウェアの挙動を記録したログから想定されるリスクを判定し，その対策行動を誘導するためのセキュリティ警告画面を表示する．本警告画面を表示するうえで必要な要件を早川ら[1]を参考に以下の 4 つに定めた．

(1)コンピュータに脅威を与えるソフトウェアの挙動が検出対象であること
(2)警告画面の内容は，ユーザに検出対象の危険性を知らせること
(3)警告画面の内容は，ユーザのセキュリティの知識が乏しくても理解できること
(4)警告画面は，ユーザが行う作業を著しく妨げないこと

以上を満たす提案手法の詳細を次に示す．

2.2 危険なソフトウェア動作

ユーザにリスクを及ぼすと考えられるソフトウェアの挙動と挙動から想定されるリスクは多数存在する．本研究では，ファイル及びレジストリに関する挙動を対象とする．要件(1)を満たす挙動を早川ら[1]伊波ら[2]を参考に定めた．尚，提案の有効性を確かめた後，対象とするソフトウェアの挙動の範囲を拡張していく予定である．

表 1 ソフトウェアの挙動と想定されるリスク

ソフトウェアの挙動	想定されるリスク
実行ファイルの作成	不正インストール
実行ファイルの書込み	ファイルの複製
実行ファイル名の変更	ファイルの複製
レジストリ書込み	OS 起動時の自動実行

2.3 セキュリティ警告画面の表示項目

提案する警告画面を図 1 に示す．警告には，以下の項目を表示する．

・検出されたソフトウェアの名前
・検出した挙動から想定されるリスク
・リスクから想定される被害例
・詳細情報参照
・ユーザの選択肢(削除)

要件(2)を満たすため，過去に報告された被害を基に作成した情報を被害例として表示する．具体的な例を用いることで，ユーザに危機意識を持たせる．

要件(3)を満たすため，デジタル証明書やマルウェアの種類といった専門用語は警告画面に表示しない．ユーザの選択肢にはソフトウェアの削除を設けた．ユーザはセキュリティ警告内容からソフトウェアに問題があると判断した場合，削除を選択する．

要件(4)を満たすため，今後も検出対象とするかをユーザに選択させる．ユーザが検出対象としないことを選択した場合は，当該ソフトウェアをホワイトリストに登録する．

A Security Warning System Associating Detected Actions with their Risks to Motivate Users to Take Countermeasures
† Izumi Nishina
† Tokushima University

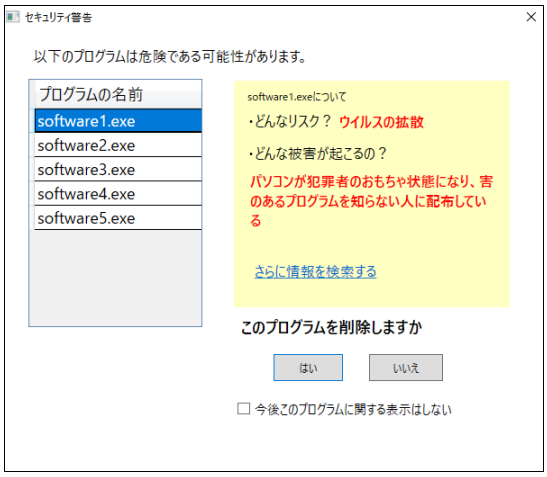

図 1　提案するセキュリティ警告のイメージ

3. 実装

提案手法の有用性を評価するため，プロトタイプシステムを 64bit の Windows 10 上に実装した．

ログの取得には，全てのプロセス処理を監視できることから，Microsoft 社の提供するツール Process Monitor を用いた．早川ら[1]，伊波ら[2]が検出対象と定義した値の組み合わせを参考に，検出対象を次のように定めた．

・Path が Windows システムフォルダなどの重要なファイルシステムやプログラムの自動実行に関係するレジストリである
・上記の Path に対してファイル作成や書き込み，レジストリキーに値を登録した実行ファイルである

最初に，提案システムは取得したログから上記条件に従い実行ファイル名や動作などを抽出しデータベースへ登録する．次に，登録された動作項目に対応するリスク及び被害例を与える．尚，動作に対応するリスクおよび被害例は予めデータベースに登録された値を用いる．最後に，データベースの情報をセキュリティ警告としてユーザに提示し，ユーザの選択に従い処理する．

4. 実験と結果

提案手法の有用性の評価を行った．

4.1 実験

被験者 12 名を対象に，仮想マシン上のゲスト OS に提案手法を実装したプロトタイプシステム及び既存手法として Windows Defender を使用してもらいセキュリティ警告に対する被験者の対応を調査した．選択行動の判断基準を明らかにするため，実験の最後に被験者へアンケート調査を行った．検出対象となるソフトウェアは，既存手法と提案手法の両者が検知できる実行可能なマルウェアである．

4.2 実験結果

セキュリティ警告を閲覧したユーザが当該ソフトウェアの削除を選択した場合，セキュリティ警告はユーザを対策行動へ誘導したと定義する．実験の結果，既存手法と提案手法ともに対策誘導率が 95%であり，対策行動の誘導に差がないことがわかった．また，既存手法でユーザが最も頼りにした情報は 12 人中 7 人が選択した「説明」であり，ソフトウェアの脅威を説明している．従来手法では 12 人中 12 人がリスクから想定される被害例を頼りにしたと回答した．

4.3 評価

提案したセキュリティ警告手法は，少ない表示項目から既存手法と同じ対策誘導率を得ることができた．また，アンケート回答では既存手法で削除に至らなかった理由として「実際に悪さをする内容ではなかったため」と記述した被験者がいた．これは，検出されたソフトウェア 5 つのうち被験者が削除しなかったソフトウェアのみ「このプログラムは危険であり」という記述がなかったためだと考えられる．提案手法では，「ありえそうなリスクだったので，パソコンなどを使うのが少し怖くなりそうになった」という記述があり，被験者は脅威を身に起こる事象として捉えることができたと考えられる．

5. おわりに

本論文では，Windows 上で，ログ情報をもとに動作とリスクから紐づけた被害例を提示するセキュリティ警告を提案した．リスクから想定される被害例は，脅威をユーザの身近な問題と感じさせ対策行動にユーザを誘導できることを確認した．

参考文献

[1]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, マルチメディア, 分散, 協調とモバイル（DICOMO2014）シンポジウム, pp. 1720-1727, Jul. 2014

[2]危険なシステムコールに着目した Windows 向け異常検知手法, 伊波靖, 高良富夫, 情報処理学会論文誌, Vol. 50, No. 9, pp. 2173-2181, Sep. 2009