7G-7

ユーザによりインストールされたソフトウェアの判別に関する検討

石沢千佳子　　佐藤　充　　西田　眞
秋田大学

1. はじめに

複数のユーザにより共同使用されるコンピュータ（以下，PC と表記する）内に，ユーザによりインストールされたソフトウェアが存在すると，これが他のソフトウェアの誤作動や不正インストールの一因となる場合がある。従って，このようなトラブルを未然に防止するため，PC 内にインストールされているソフトウェアを点検し，ユーザによりインストールされたソフトウェアを発見することが管理者に求められている[1][2]。

そこで本研究では，大学のコンピュータ実習室に設置された PC（OS : Microsoft Windows®）を対象とし，PC 内に存在するソフトウェアの中から，ユーザにより新規にインストールされたソフトウェアを判別可能とする手法を提案し検討を加えた。

2. 提案手法

2.1 概要

本研究では，全てのソフトウェアに実行形式ファイルが含まれていることに着目し，実行形式ファイルをソフトウェアと見なした。すなわち，本研究では，実行形式ファイルを検出してソフトウェアの判別を行う。

本研究で提案する手法の流れを図 1 に示す。はじめに，ユーザによる PC 使用前に PC 内にインストールされているソフトウェアの実行形式ファイルの検出を行い，これを「使用前情報」として保存する。次に，ユーザが PC 使用時に起動した実行形式ファイルを「実行ログ」として記録する。ユーザによる PC 使用後，PC 内の実行形式ファイルを再検出し，「使用後情報」として保存する。最後に，「使用前情報」と「実行ログ」並びに「使用後情報」の比較を行い，ユーザにより新規インストールされたソフトウェアの判別を行う。

2.2 ソフトウェアの検出処理

PC 内の実行形式ファイルの検出には，ファイルのヘッダ情報を用いた。これは，ヘッダ情報の変更が困難であるため，ファイル名を変更しソフトウェアを隠蔽するような事例に対しても対処可能と判断したためである。なお，実行形式ファイルには DLL ファイルと呼ばれる単体では実行不可能なものもあるため，DLL ファイルは検出対象から除外している。

2.3 ソフトウェアの使用履歴作成処理

ユーザによりインストールされたソフトウェアは，インストール後，使用される可能性の高いことが予想される。従って，ユーザが使用したソフトウェア，すなわち実行された実行形式ファイルと「使用前情報」を比較することで新規ソフトウェアの判別が可能となる。また，実行された実行形式ファイルを記録しておくことにより，インストールされたソフトウェアが使用後に削除されてしまった場合においても，新規ソフトウェアが存在していたことを把握可能となる。

そこで，PC 使用中にユーザが実行した実行形式ファイルを記録するプログラムを常時起動させ，「実行ログ」を作成した。

2.4 新規ソフトウェアの判別処理

判別処理の流れを図 2 に示す。新規ソフトウェアの判別には，ファイル ID と呼ばれるファイル識別子を用いた。ファイル ID は，PC 内の全てのファイルに割り当てられる固有の値であり，ファイルの実行等による値の変更はない。従って，PC 使用前後において同じ値のファイル ID を持つ実行形式

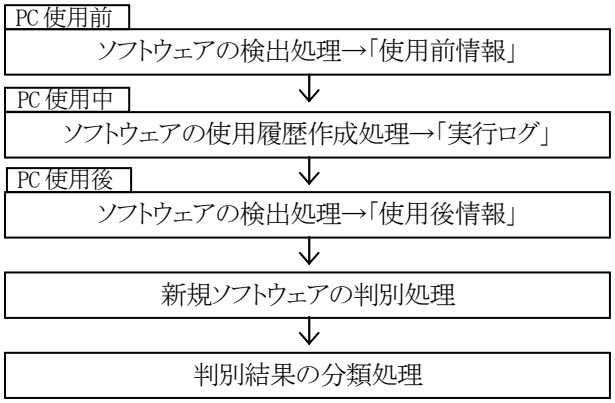

図 1 提案手法の流れ

A Study of Techniques to Distinguish Softwares Installed in the Computer System by Users
Chikako Ishizawa, Mitsuru Sato and Makoto Nishida
Akita University

ファイルは既存のソフトウェアであると判別が可能である。また，PC 使用前に存在しない新たな値のファイル ID を持つ実行形式ファイルは新規にインストールされたソフトウェアであると判別が可能である。さらに，「実行ログ」を判別処理に付加することにより，ファイル実行の有無の区別も可能となる。そこで，PC 使用前後の情報と実行ログを用いて判別を行った。

2.5 判別結果の分類処理

コンピュータ実習室のシステム管理者にインタビューしたところ，PC から検出される実行形式ファイルには「OS のアップデート等により特定のフォルダに作成されるファイル」が含まれること，並びに「授業で使用するためユーザによるインストールを許可したソフトウェア」と「個人使用を目的として許可なくインストールされたソフトウェア」に分類されること等の知見が得られた。

そこで提案手法では，管理者にとって必要な「個人使用を目的としてインストールされたソフトウェア」に関する情報を得るため，判別処理によって得られた結果に対し分類処理を施した。分類処理の流れを図 3 に示す。

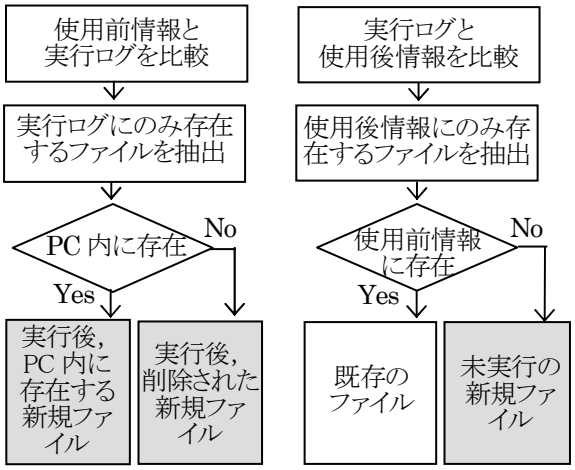

図 2　判別処理の流れ

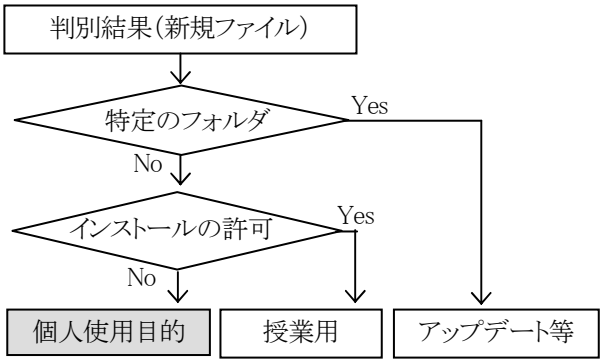

図 3　分類処理の流れ

3. 実験結果およびまとめ

はじめに，実行形式ファイルを検出してソフトウェア判別を行うことの有用性を検討するため，被験者により新規インストールされたソフトウェアを対象とし，実行形式ファイルの検出を行った。提案手法と手動により検出した結果を表 1 に示す。手動による結果同様，提案手法は新規インストールされたソフトウェアに含まれる全ての実行形式ファイルを検出可能であった。

次に，秋田大学工学資源学部情報工学科コンピュータ実習室 I における 60 台の PC（PC-1～PC60）を対象とし，提案手法を用いた新規ソフトウェアの判別および分類を行った。具体的には，それぞれの PC において判別までの各処理を実行し，管理者用 PC で判別結果を収集し分類処理を施した。得られた結果の一例を表 2 に示す。PC-1 の結果は，手動で確認した結果と一致し，ユーザによりインストールされたソフトウェアが適切に判別および分類されていることを示している。

以上の結果は，本研究で提案する新規インストールソフトウェア判別法が有用であることを示唆している。

表 1　実行形式ファイルの検出結果

インストールされたソフトウェア数	提案手法	手動検出
	検出された新規ファイル数	ソフトウェアに含まれる実行形式ファイル数
5	10	10

表 2　判別・分類結果例（PC-1）

	実行済みの新規ファイル数	未実行の新規ファイル数
個人使用目的のソフトウェア	0	5
インストールの許可されたソフトウェア	3	13
アップデート等に関するソフトウェア	2	43
合計	5	61

参考文献

[1]高橋俊成：「ソフトウェアの利用管理の難しさ（情報セキュリティ辞典）」，共立出版，pp. 430-431 (2003)

[2]社団法人コンピュータソフトウェア著作権協会，http://www2.accsjp.or.jp/