4V-9

ログ情報およびヘッダー情報を用いたインストールソフトウェア判別法の開発

佐藤　充　　石沢　千佳子　　西田　眞
秋　田　大　学

1. はじめに

筆者らはこれまでに、ユーザによりインストールされたソフトウェアの有無を判別する手法の開発を目的とし、コンピュータ（以下、PC と表記）内に記録されている実行形式ファイルを、ユーザがインストールしたソフトウェアに含まれるものと既に存在していたものとに分類する手法を提案した[1]。その結果、全ての実行形式ファイルを適切に分類可能であることが明らかとなった。

しかしながら、ファイルのヘッダー情報を用いて実行形式ファイルを検出する場合、単体では実行不可能であるため判別対象外となるファイルも検出してしまう点が課題として残された。そこで、この不要ファイルの検出を防止するため、ヘッダー情報に加え PC 使用状況の記録（以下、ログと表記）を用いた実行形式ファイルの検出処理を提案する。

2. 提案手法

2.1 概要

提案手法の流れを図 1 に示す。始めに PC 内に記録されている実行形式ファイル全ての検出を行った。次にユーザによる PC 使用状況を監視し、使用された実行形式ファイル名をログとして記録した。PC 使用後、得られたログと PC 使用前のファイル情報を比較し、ユーザが実行した新規ファイルを判別した。さらに、PC 内に記録されている実行形式ファイルを再検出し、PC 使用前後の実行形式ファイルの情報を比較することでユーザが実行しなかった新規ファイルの判別を行った。

Development of a technique using log and header information to distinguish softwares installed in the computer system
Mitsuru Sato, Chikako Ishizawa and Makoto Nishida
Akita University
1-1, Tegata Gakuen-Machi, Akita City.
010-8502 Japan

2.2 PC 使用状況の監視処理

ユーザによりインストールされたソフトウェアは、インストール処理直後に使用される可能性が高いと予想される。従って、ユーザが実行したファイルを検出し、PC 使用前に検出した実行形式ファイルの情報と比較することで、不要なファイルを検出することなく、ソフトウェアの判別が可能と考える。そこで、PC の使用状況を監視し、ユーザが実行したファイルを検出した。具体的には、ユーザが実行する実行形式ファイルを記録するプログラムを常時起動し、実行したファイルの情報をログに記録した。

2.3 実行形式ファイルの検出処理

PC 内の実行形式ファイルの検出には、ファイルのヘッダー情報を用いた。ヘッダー情報は利用者による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 対処可能であると考える。 なお、 実

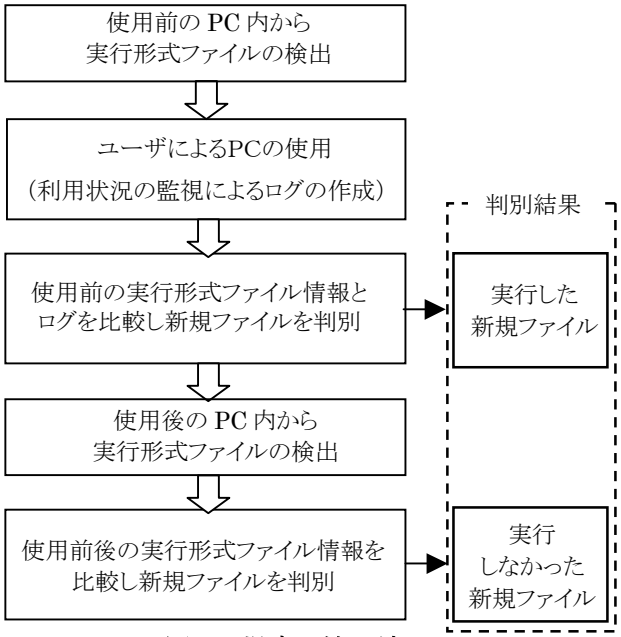

図 1　提案手法の流れ

行形式ファイルには「DLL ファイル」と呼ばれる種類があるものの、単体では実行不可能であるため、ヘッダー情報を用いて DLL ファイルを検出対象から除外した。また、PC 使用後の検出処理では、インストール処理のみが行われ実行されなかった新規ファイルの判別を行うため、ログに含まれるファイルも除外した。

2.4 実行形式ファイルの判別処理

新規にインストールされた実行形式ファイルの判別は、ファイル ID の比較により行った。ファイル ID とは、全てのファイルに割り当てられる固有の値であり、ファイルの実行による値の変更はない。このため、ファイル ID が同一のファイルは予め記録されていたファイルに分類され、新たなファイル ID を持つ実行形式ファイルが、ユーザによって新規インストールされたソフトウェアに含まれるファイルに分類される。

3. 検証実験および結果

ログおよびヘッダー情報を用いた検出処理の有用性を検証するため、ヘッダー情報のみを用いた検出処理との比較を行った。具体的には、ユーザによって PC 内にインストールされた 5 本のソフトウェアに含まれる実行形式ファイルを、それぞれの処理を用いて判別する実験を行った。実験結果を表 1 および表 2 に示す。ログおよびヘッダー情報を用いた検出処理は、不要なファイルを含めることなく、判別対象の実行形式ファイルのみを検出していることが分かる。また、ヘッダー情報のみを用いた検出処理と比較し、判別時の比較ファイル数が約 60%減少しており、これに伴い処理時間も約 60%短縮していることを確認した。以上の結果は、ログおよびヘッダー情報を用いた検出処理が有用であることを示唆するものである。

4. ネットワークシステムへの適用

ネットワークを介して複数台の PC を調査することにより、点検作業の効率が向上し PC 管理者の負担が軽減されると予想される。そこで、ネットワーク接続された PC16 台（PC-1～PC-16）に対し提案手法を適用した。具体的には図 2 に示すようなネットワークシステムにおいて、クライアント PC 側で提案手法の処理を実行し、管理者 PC は分類結果のみを収集する形式とした。なお、クライアント PC 側で実行される実行形式ファイルの検出処理および判別処理は Microsoft Windows ® に標準搭載されている「タスクスケジューラ機能」を用いて一定間隔で自動的に行った。

上記の処理を施した各クライアント PC を複数のユーザにより一週間使用してもらい、得られた結果を管理者 PC が収集した。各クライアント PC における処理結果を管理者 PC で収集可能であることが明らかとなった。結果の一部として PC-1 で得られた結果を表 3 に示す。

表 1　検出結果の比較

インストールしたソフトウェア数	ヘッダー情報のみを用いた検出		ログとヘッダー情報を用いた検出	
	検出された実行形式ファイル数	検出された不要な実行形式ファイル数	検出された実行形式ファイル数	検出された不要な実行形式ファイル数
5	10	6	10	0

表 2　ファイル数の比較

検出処理	PC 使用前のファイル情報と比較を行うファイル	ファイル数
ヘッダー情報のみ	PC 使用後のファイル情報	14,198
ログとヘッダー情報	実行されたファイルのログおよび PC 使用後のファイル情報	5,388

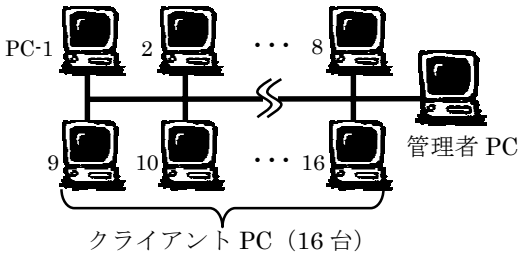

図 2　ネットワークを介したシステムの概観

表 3　クライアント PC　PC-1 の結果

インストールされたソフトウェア数	ソフトウェアに含まれる実行形式ファイル数	検出された実行形式ファイル数
3	12	12

参考文献

[1]石沢　千佳子・西田　眞・淀川　東司朗、「ファイル情報を用いたインストールソフトウェア判別法の検討」、平成 15 年度電気関係学会東北支部連合大会、No.1H-1