USBメモリを用いて持ち出されたファイルの置き忘れ検出に関する検討

安藤 優　　石沢 千佳子　　西田 眞

秋田大学

1.はじめに

コンピュータ内に保存されている情報の漏洩が社会的に大きな問題となっている。具体的には、自宅や顧客先での使用を目的とし、組織構成者によって持ち出されたファイルを持ち出し先である自宅等のPC（以下、持ち出し先PCと表記する）から漏洩してしまう場合の多いことが報告されている[1][2]。このような漏洩は、「ファイルにアクセス可能な者が持ち出しを行っていること」や「持ち出し先PC内に残されたファイルの取り扱いはPC所有者のモラルに委ねられること」、「持ち出し先PCのセキュリティを管理することは不可能であること」等に起因しており、完全な防止が困難である。このため、持ち出し先PC内にファイルを置き忘れないことが重要であると考える。

そこで本研究では、持ち出し先PCに対するファイルの置き忘れの有無を検出する手法の開発を目標とする。基礎研究として、USBメモリを用いて持ち出されたファイルに対して行われた操作のログ（以下、操作ログと表記する）を取得し、この操作ログを解析することにより持ち出し先PC内へのファイルの置き忘れを検出する手法を検討した。

2.ファイルインデックスの変化

USBメモリ内のファイルを持ち出し先PCへコピーした場合、持ち出し先PCのフォルダ内にファイルが新規作成される。フォルダ内のファイルはファイルインデックスにより管理されている。このため、図1に示すように、ファイルのコピーや削除などのファイル操作に対応してファイルインデックスへファイル名の登録や削除が行われる。

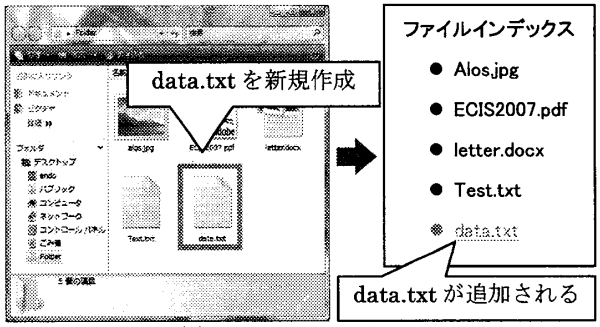
そこで本研究では、ファイルインデックスの変化をファイル操作のログとして取得し、ファイルの置き忘れを検出する手法について検討する。

3.提案手法

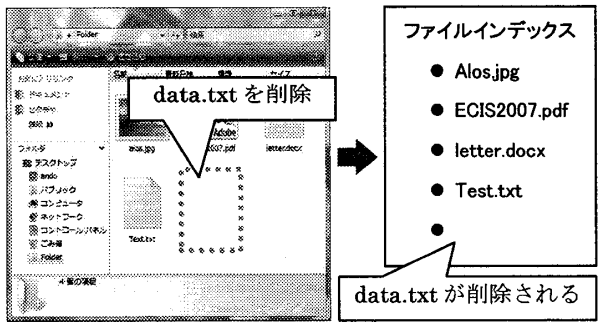
3.1 概要

本研究が想定するシステムの概要を図2に示す。本研究では、持ち出し先PCが組織外のPCである場合を想定している。このため、ファイルインデックスの変化情報を取得するためのプログラム（以下、検出プログラムと表記する）を、持ち出し先PCへインストールすることは不可能である。

そこで提案手法では、ファイルの持ち出しに使用するUSBメモリ内に検出プログラムを予め記録しておき、USBメモリが持ち出し先のPCに接続された時に自動起動させて操作ログの取得を行った。さらに、USBメモリが取り外された時、取得した操作ログを解析し、持ち出し先PCへのファイルの置き忘れを検出した。また、置き忘れが検出された場合、PC上でユーザに警告を発し、ファイルの削除を促す。なお、本研究ではファイルの持ち出しに際して、検出プログラムが記録されているUSBメモリのみが使用可能であること、Microsoft Windowsが搭載されているPCを使用することを前提として検討を加えた。



(a)新規作成の場合



(b)削除の場合

図1　ファイル操作とファイルインデックス

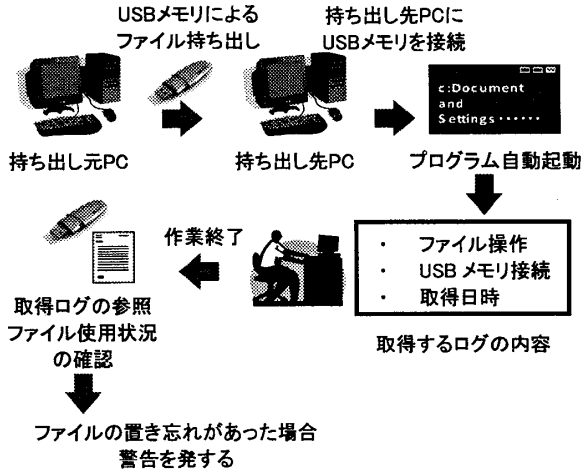


図2　想定するシステムの概要

Study on Detection of Files Carried by Using USB Memory.
Yuu Andoh, Chikako Ishizawa and Makoto Nishida (Akita Univ.)

3.2 操作ログの取得

操作ログの取得、すなわちファイルインデックスの変化情報の取得にはAPI(Application Program Interface) [3]を用いた。具体的には、USBメモリが持ち出し先PCに接続されている間、ファイルインデックスの変化を監視し、新規作成および削除の変更があった場合に、「新規作成ログ」、「削除ログ」をそれぞれUSBメモリ内のログファイルに記録する。記録する内容は、“変更の種類、時刻、ファイル名およびパス、アカウント名、PC名”である。

さらに、操作ログを取得するプログラムが起動した際に、その時刻を「プログラム起動ログ」として記録する。提案手法で取得する操作ログの種類を表１に示す。

3.3 置き忘れの検出

ファイルの置き忘れを検出する処理の流れを図３に示す。コピーの行われたことを示す「新規作成ログ」と削除の行われたことを示す「削除ログ」が対になっていない場合、持ち出されたファイルは置き忘れられたと判断する。

作業中に、USBメモリが物理的に取り外された場合、ログを取得できない期間が存在し、その間にファイル操作の行われる可能性がある。例えば、USBメモリが取り外されている間に、２次コピーが行われる場合もあり得る。そこで提案手法では、「プログラム起動ログ」に着目しUSBメモリが取り外されている期間を検出した。具体的には、「新規作成ログ」と「削除ログ」の間に「プログラム起動ログ」が存在する場合、置き忘れられた可能性があると判断する。以下、置き忘れられた可能性のある操作を「不正操作」、置き忘れられた可能性のない操作を「正規操作」とそれぞれ表記する。

4.実験

提案手法の有用性を検討するため、以下の実験を行った。なお、被験者は３名である。

実験１：正規操作の検出
- ① USBメモリをPCに接続し、ファイルをPC上へコピーする。
- ② コピーされたファイルを削除し、USBメモリをPCから取り外す。

実験２：不正操作（ファイルの置き忘れ）の検出
- ① USBメモリをPCに接続し、ファイルをPC上へコピーする。
- ② USBメモリをPCから取り外す。

実験３：不正操作（USBメモリの再接続）の検出
- ① USBメモリをPCに接続し、ファイルをPC上へコピーする。
- ② USBメモリをPCから取り外す。
- ③ PC上のファイルをコピーする（２次コピー）。
- ④ 再度、USBメモリをPCに接続する。
- ⑤ 手順①でコピーされたPC上のファイルを削除し、USBメモリをPCから取り外す。

5.実験結果および検討

被験者３名が実験１～実験３を行ったところ、いずれの実験においても、取得した「新規作成ログ」、「削除ログ」、「プログラム起動ログ」の対応関係から、正規操作および不正操作をそれぞれ検出することが可能であった。取得した操作ログの一例を図４に示す。このことは、３種類の操作ログを持ち出し先のPCから取得することにより、置き忘れられたファイルが検出可能であることを示唆している。

表１ 操作ログの種類

操作ログ名称	持ち出し先 PC における操作	ログの情報
新規作成ログ	USB メモリ内のファイルをコピー	ファイル名 作成時刻
削除ログ	ファイルを PC から削除	ファイル名 削除時刻
プログラム起動ログ	USB メモリを接続	起動時刻

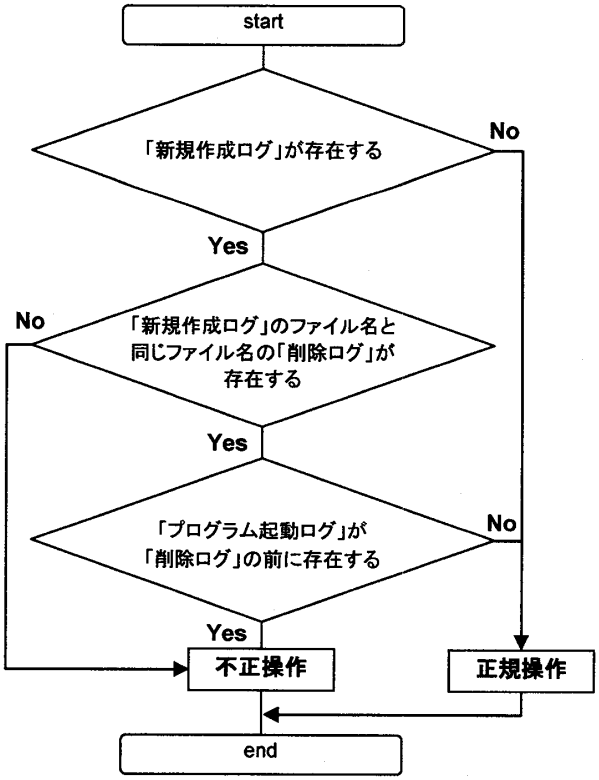


図３ 検出処理の流れ

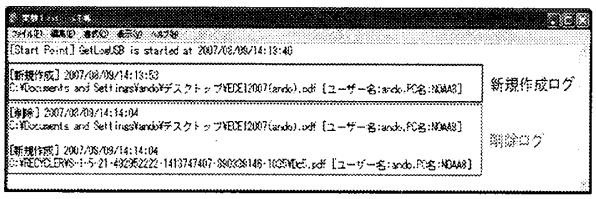


図４ 取得した操作ログの一例

参考文献

[1]2006 年度　情報セキュリティインシデントに関する調査報告書，NPO 日本ネットワークセキュリティ協会（2007）

[2]情報漏えいインシデント対応方策に関する調査報告，独立行政法人情報処理推進機構（2007）

[3]MSDN ライブラリ http://msdn2.microsoft.com/