L-034

クリップボード監視処理を用いたコピー操作ログ取得法
Method to Get Logs of Copy Operations by Monitoring Processing of Clipboard

佐藤 諒† 石沢 千佳子† 西田 眞†
Ryo Sato Chikako Ishizawa Makoto Nishida

1. はじめに

近年，組織の管理が及ばない自宅などの私有 PC に機密データをコピーし，そのまま PC 内にデータを残していたために，データの漏洩した事例が多数報告されている[1]. このため，情報漏洩の未然防止には，組織の管理下にない外部の PC（以下，持ち出し先 PC）内に，機密データを残さないことが重要と考える.

筆者らはこれまでに，USBメモリなどの可搬記録媒体を用いて持ち出されたファイルが持ち出し先PC内に残留することを防止するため，持ち出し先PC上で行われたファイル操作に対するログを取得し，このログを解析することによってファイルの残留を検出する手法（以下，残留ファイル検出法）の開発を目標として検討を加えてきた. その結果，Microsoft® Windows®標準のファイルブラウザであるExplorer®を介したコピー操作を全て検出可能であることを明らかにした[2]. しかしながら，Explorer®を介さないコピー操作を検出するまでには至っていない. そこで本稿では，“可搬記録媒体内のファイルをアプリケーションソフトウェアを用いて開き，データの一部を持ち出し先PC内にコピーする”という操作（以下，アプリケーションソフトウェアを介したコピー操作）の検出を目的としたログ取得方法について検討を加えた.

2. 残留ファイル検出法の概要

本研究で目標とする残留ファイル検出法の概要を図 1 に示す.

残留ファイル検出法では，一連の処理を実行するプログラムをUSBメモリ内に予め格納しておき，持ち出し先PCに接続された時にプログラムを起動させる. 次に，ログの取得を行い，残留ファイルを検出する. なお，持ち出し先 PCには，Microsoft® Windows® XP，Microsoft® Windows® 7 のOSが搭載されていることを前提条件とする.

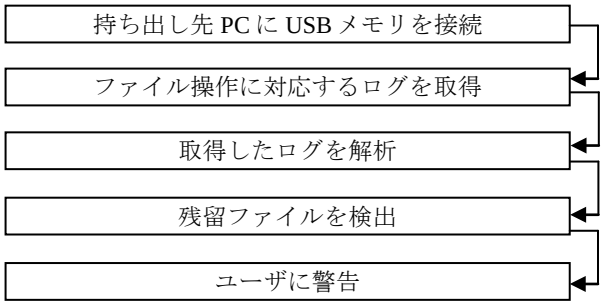


図 1 残留ファイル検出法の流れ

†秋田大学 Akita University

3. クリップボード監視処理を用いたログ取得方法

“アプリケーションソフトウェアを介したコピー操作”が行われた場合，Microsoft® Windows®では，クリップボードと呼ばれるメモリ領域にコピー対象データが一時的に保存された後，コピー先のファイルが更新される. そこで本研究では，クリップボードの内容変更を検知するための監視処理，並びに更新ファイルの特定に必要な情報の記録処理を併用したログ取得方法を提案する.

3.1 クリップボード監視処理

クリップボード監視処理では，クリップボードビューアチェイン[3]と呼ばれるクリップボードの変更通知受信機構に，自作の監視処理プログラムを登録し監視を行う. クリップボードの内容が変更された場合，変更通知を受信した時刻をログに記録する.

3.2 更新ファイルに関する記録処理

Microsoft® Windows®では，ファイルインデックスを用いてファイルを管理しており，ファイルインデックスに登録されているファイル名や作成日時などの情報がファイル操作に対応して変更される[3]. 従って，ファイルインデックスの変更状況に基づいて，更新ファイルの特定が可能と考える.

一方，PC 上でファイル操作が行われた場合，ファイル操作に対応する API 関数が実行される[3]. 従って，API 関数に基づいた更新ファイルの特定も可能と考える.

そこで，更新ファイルの特定に必要な情報を記録する処理として，次の 2 種類の処理を提案する.

(1)ファイルインデックスの変更履歴記録処理:ファイルインデックスを監視し，変更種別，コピー先ファイルのパス，並びにファイルのハッシュ値をログに記録する[2].

(2)API 関数の実行履歴記録処理:API 関数の実行状況を監視し，API 関数名，コピー元およびコピー先ファイルのパスをログに記録する.

本稿では，上記処理（1）とクリップボード監視処理（3.1 節参照）を併用した方法を“提案手法 A”とする. 一方，上記処理（2）とクリップボード監視処理（3.1 節参照）を併用した方法を“提案手法 B”とする.

4. 実験

4.1 実験手順

クリップボード監視処理を用いたログ取得方法の有用性を検証するため，提案手法Aおよび提案手法Bを用いてファイル操作に対するログをそれぞれ取得し，解析を行った. 実験に用いたファイル操作は，USBメモリ内のファイルに対する“コピー”，“名称変更”，“更新”，“移動”，“削除”，並びに“アプリケーションソフトウェアを介したコピー操作”の 6 種類の操作を組み合わせ

た 89 通りの操作とした．また，実験にはMicrosoft® Windows® XP Professional，並びにMicrosoft® Windows® 7 Professionalの搭載されたPC（2 台），およびメモ帳（Microsoft® Windows®標準のテキストエディタ）を用いた．

4.2 実験結果および考察

実験の結果，Microsoft® Windows® XP搭載のPCを用いた場合は，提案手法Aおよび提案手法Bのどちらの手法においても全ファイル操作（89 通り）に対するログの取得が可能であった．しかしながら，Microsoft® Windows® 7 搭載のPCを用いた場合は，提案手法Bにおいて“移動”および“名称変更”以外のファイル操作に対するログ（73 通り）の取得が不可能であった．これは，Microsoft® Windows® XPとMicrosoft® Windows® 7 では，実行されるAPI関数が異なるためと推測される．

提案手法 A・B によるログを比較したところ，提案手法 B によるログには，実験で行ったファイル操作以外のログが多数記録されていた．一方，提案手法 A によるログには，実験で行ったファイル操作に対するログのみが記録されていた．そこで，実験で行ったファイル操作のみに着目して解析を行うため，提案手法 A によるログを解析に用いた．

ログの解析結果例を図 2 に示す．“アプリケーションソフトウェアを介したコピー操作”が行われた場合，クリップボードの内容が変更された後（図 2 太線枠内参照），ファイルインデックスの変更種別が“更新”または“新規作成”であるログを取得していることがわかる（図 2 点線枠内参照）．そこで，クリップボードの内容変更後に取得された“更新”および“新規作成”のログのみを抽出したところ，持ち出し先 PC 内の既存ファイルに対する“アプリケーションソフトウェアを介したコピー操作”を全て検出可能であることが明らかとなった．この結果は，ファイルインデックスの変更種別の順序に基づいて“アプリケーションソフトウェアを介したコピー操作”を検出可能であることを示唆している．今後は，図 3 に示す解析手法を用いた解析結果について検討を加える予定である．

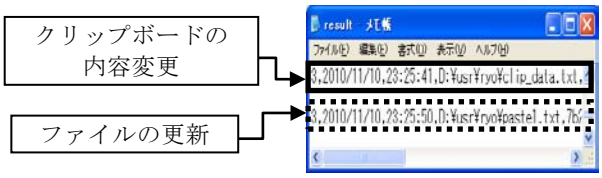
なお，クリップボードの内容が変更された後に取得される“新規作成”のログの検出に関しては，使用されるアプリケーションソフトウェアごとに取得されるログが異なるため，さらなる検討が必要である．

5. おわりに

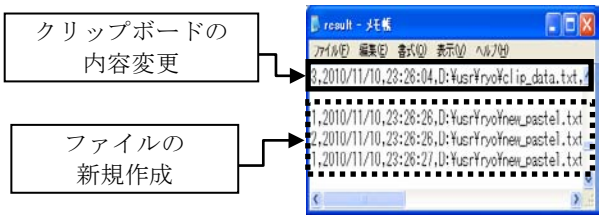
本研究では，“アプリケーションソフトウェアを介したコピー操作”の検出を目的とし，残留ファイル検出法におけるログ取得方法について検討を加えた．得られた成果を以下にまとめる．

(1)クリップボードの内容変更のタイミングとユーザの行うファイル操作には，関連があることを明らかにした．

(2)“ファイルインデックスの変更履歴記録処理とクリップボード監視処理を併用した手法”を用いて取得されたログをファイルインデックスの変更種別の順序に着目して解析することは，“アプリケーションソフトウェアを介したコピー操作”を検出可能にすることを明らかにした．



(a) 既存ファイルに対するアプリケーションソフトウェアを介したコピー操作



(b) 新規作成されたファイルに対するアプリケーションソフトウェアを介したコピー操作

図 2　ログ解析結果例
(Microsoft® Windows® XP Professional)

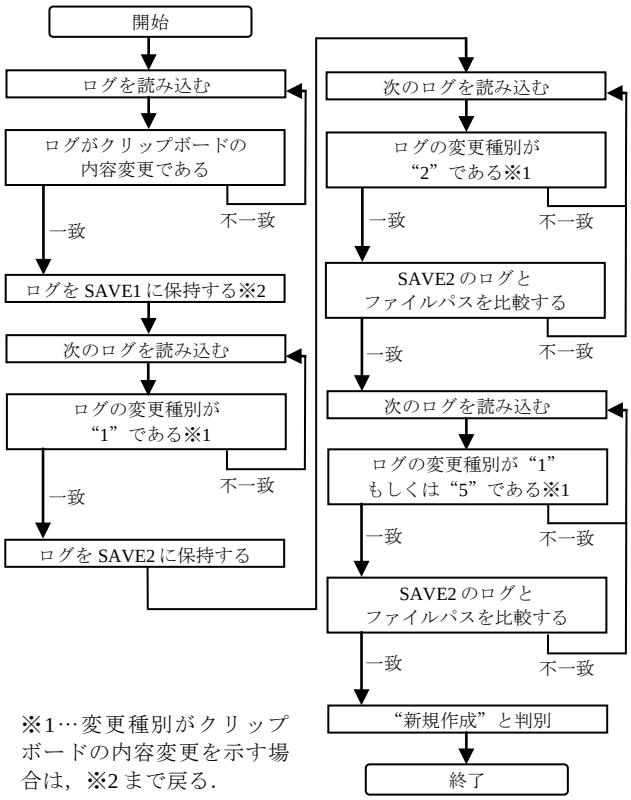


図 3　“新規作成”のログを対象とした解析手法の流れ

参考文献

[1]NPO 日本ネットワークセキュリティ協会, “2009 年情報セキュリティインシデントに関する調査報告書 Ver 1.1” (2010).

[2]石沢 千佳子, 安藤 優, 西田 眞, “ディレクトリの変更履歴およびハッシュ値に基づいた残留ファイル検出手法”, 電気学会論文誌 C, Vol.130, No.11, pp.2074-2083 (2010).

[3]MSDN ライブラリ, http://msdn.microsoft.com/ja-jp/library/