5Z-8

可搬記録媒体からPC内にコピーされた残留ファイルの検出手法の開発

佐藤 諒　　石沢 千佳子　　西田 眞

秋田大学

1.背景・目的

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の PC 内に残留することは，情報漏洩の脅威になり得る[1]．筆者らはこれまでに，ファイルそのものが PC 内にコピーされた場合にディレクトリ[2]の変更履歴を用いることによって，残留ファイルを全て検出可能であることを明らかにした[3]．しかしながら，ファイル内のデータがコピーされた条件下では，コピーデータを含む残留ファイルを検出するまでには至らなかった．そこで本稿では，“可搬記録媒体に存在するファイル内のデータの一部を PC にコピーする操作（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）”の検出方法について検討を加えた．なお，本研究では，Microsoft® Windows® XP および Microsoft® Windows® 7 の OS が搭載されている PC の使用を前提条件とする．

2.ログ取得処理に関する検討

2.1 ログ取得処理

“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[2]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とファイルの更新を検知するため，クリップボードとディレクトリの状態を監視してログを取得し，ディレクトリの変更種別，ファイルパス，並びにハッシュ値を USB メモリ内のログファイルに記録する．

2.2 実験方法および結果

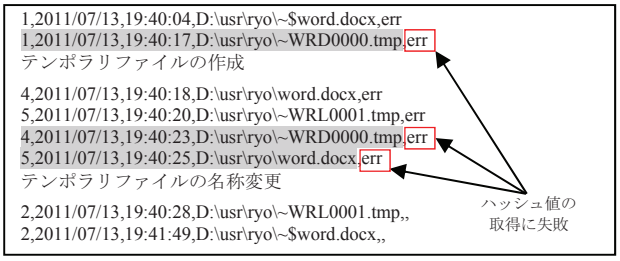
アプリケーションソフトウェアごとに取得されるログの相違を検証するため，ログ取得処理を用いて，“更新”および“新規作成”の各ファイル操作に対応するログを取得した．実験に用いたアプリケーションソフトウェアおよび OS の詳細を表 1 に示す．

取得ログの例を図 1 に示す．実験の結果，アプリケーションソフトウェアごとに異なるログが取得された．また，メモ帳以外のアプリケーションソフトウェアでは，ファイルの編集中にテンポラリファイルのハッシュ値を取得することは不可能であることがわかった．

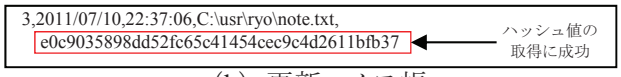
しかしながら，コピー先のファイルが更新された場合，いずれのアプリケーションソフトウェアを用いた場合においても，“ファイルの更新”，“ファイルの追加”，並びに“テンポラリファイルの作成および名称変更”のうち，いずれかのログが取得されることが明らかとなった．従って，クリップボードの内容変更後に記録されたログを調査することは，“アプリケーションソフトウェアを介したコピー操作”を検出可能にすると考える．

表 1　実験対象アプリケーションソフトウェアおよび Microsoft® Windows®の種別

Microsoft® Windows® XP Pro.	Microsoft® Windows® 7 Pro.
Word2003,Word2007	Word2007,Word2010
Excel2003,Excel2007	Excel2007,Excel2010
PowerPoint2003, PowerPoint2007	PowerPoint2007, PowerPoint2010
メモ帳	メモ帳



（a）更新 : Word2010



（b）更新 : メモ帳

図 1　取得ログ例（Microsoft® Windows® 7 Pro.）

3.ログ解析処理に関する検討

3.1 ログ解析処理

ログ解析処理では，ディレクトリの変更種別とファイル名を調査し，コピー先ファイルの更新処理に対応するログ（2.2 節参照）を検出した後，ディレクトリの変更種別に基づき，ファイルのトレースを行う．

3.2 実験方法および結果

ログ解析処理の有用性を検討するため，“アプリケーションソフトウェアを介したコピー操作”の実行後に，“コピー，名称変更，更新，移動，削除”の操作のうち，2 種類の操作が行われた場合のログを取得し，残留ファイルの検出を行った（全 52 通り）．実験には，Word2010 およびメモ帳，並びに Microsoft® Windows® 7 Pro.が搭載さ

Development of a Method to Detect Remaining Files Copied to a Personal Computer from Portable Storage Media.
Ryo Sato, Chikako Ishizawa and Makoto Nishida
(Akita University)

れた PC を用いた．また，ファイル操作には Explorer®を用いた．

実験の結果，全 52 通りのファイル操作において，残留ファイルを正しく検出可能であることが明らかとなった．このことは，コピー先ファイルの更新処理およびディレクトリの変更種別に基づき，“アプリケーションソフトウェアを介したコピー操作”が検出可能であることを示唆している．

4.提案手法の有用性に関する検討

4.1 提案手法

従来法[3]では，USB メモリ内のファイルと PC 内のファイルのハッシュ値を比較し，残留ファイルの判別を行っている．しかしながら，“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，データのコピー先ファイルは USB メモリ内に存在しないため，ハッシュ値の比較を行うことは不可能である．このため，従来法では“アプリケーションソフトウェアを介したコピー操作”によるコピー先ファイルの残留検出が不可能であった．そこで提案手法では，“ファイルそのものをコピーする操作”および“アプリケーションソフトウェアを介したコピー操作”のどちらの操作が行われた場合であってもコピー先ファイルの残留検出を可能にするために，従来法のログ取得処理およびログ解析処理に改良を加える．具体的には，トレースのための新たな識別子としてファイル ID[2]をログファイルに追加記録し，ディレクトリの変更履歴，ファイルパス，ハッシュ値，並びにファイル ID を用いてファイルのトレースを行う．ファイル ID とは，PC 内の全ファイルに割り当てられる一意の値である．すなわち，同一のファイル ID を有するファイルは PC 内に存在しないため，ファイル ID に基づいてファイルをトレースすることが可能と考える．提案手法によって取得されるログの例を図 2 に示す．

4.2 実験方法

実際の使用状況下における提案手法の有用性を検討するため，以下に示す条件下で提案手法の搭載された USB メモリを使用してファイル操作を行った．

- 予め USB メモリ内に保存してあるファイルを使用すること
- USB メモリ内のファイルを更新しないこと
- はじめに，USB メモリ内のファイルを Explorer®またはアプリケーションソフトウェアを介して PC 内にコピーすること
- “アプリケーションソフトウェアを介したコピー操作”を実行する場合，PC 内の既存ファイルへコピーすること
- ファイル名およびフォルダ名に全角文字を使用しないこと
- USB メモリの取り外しを一連の操作の区切りとし，一連の操作を 5 回行うこと

実験には Word2010，Excel2010，PowerPoint2010，並びにメモ帳によって作成された 4 種類のファイルおよび Microsoft® Windows® 7 Pro.が搭載された PC を用いた．なお，被験者は日常的に PC を使用している 20 代の大学生および大学院生合計 5 名とした．

4.3 実験結果および考察

被験者 5 名によって行われたファイル操作を整理した結果，25 通りのファイル操作が行われたことが明らかとなった．しかしながら，全 25 通りのファイル操作のうち，9 通りの操作には指定した条件以外の操作（例えば，“アプリケーションソフトウェアを介したコピー操作”によってデータをコピーし，新規ファイルに保存するなど）が含まれていたため，これを評価の対象外とし，16 通りの操作を評価対象とした．

実験の結果，評価対象とした 16 通りの操作のうち，15 通りの操作において残留ファイルを正しく検出可能であることが明らかとなった．例えば，複数のファイルを PC 内にコピーし，名称変更や移動といった操作が行われた場合に残留ファイルを検出可能であった．

以上の結果は，提案手法を用いて残留ファイルの検出を行うことは，3 章で検証した各種ファイル操作（“アプリケーションソフトウェアを介したコピー操作”，“コピー，名称変更，更新，移動，削除”）が無作為に組み合わさって実行された場合においても，残留ファイルを正しく検出可能であることを示唆している．

一方，残留ファイルの検出に失敗した操作では，残留ファイルが含まれるフォルダを圧縮する操作が行われていた．そこで，圧縮操作を行った際に取得されるログを解析した結果，2 章で検証したログとは異なるパターンのログが取得されることが明らかとなった．また，圧縮操作によって生成されたファイルは，USB メモリ内のファイルとは異なるハッシュ値を持つため，残留ファイルの検出に失敗したと考える．従って，ファイルおよびフォルダの圧縮操作に対応したトレース方法について検討を加えることが今後の課題である．

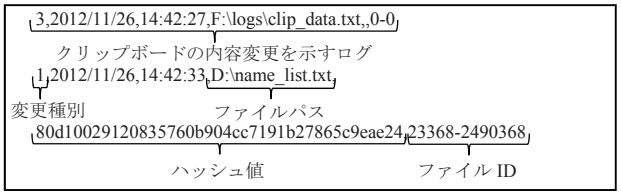


図 2　提案手法によるログの例

参考文献

[1] NPO 日本ネットワークセキュリティ協会：“2011 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～ 第 1.2 版”(2012)

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

[3] 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の検出手法”，電気学会論文誌 C，Vol.130，No.11，pp.2074-2083(2010)