Computer Security Symposium 2017
23 - 25 October 2017

Windows PC向け最小証拠保全システムの試作

長井 健[1]　上原 哲太郎[2]

概要：インシデント・レスポンスの現場においては，証拠保全は極めて重要である．しかし PC においてはストレージ容量の増大に伴い証拠保全に必要な時間の増大が問題になっている．本発表では Windows PC における NTFS を題材にして証拠保全に最低限必要な領域について検討し，最小の領域のみ保全するようにしたシステムについて報告する．

キーワード：インシデント・レスポンス，証拠保全，NTFS

A prototype system to preserve reduced e-evidence from Windows PCs

Ken Nagai[1]　Tetsutaro Uehara[2]

Abstract: It is highly important at the scene of incident-response to preserve the e-evidence. However, with the increase in storage capacity of PCs, evidence preservation becomes harder as it has become quite time consuming. In this paper, we have focused on preserving e-evidence of NTFS on Windows PCs and discusses about the minimum required area for evidence preservation in the storage. A prototype system to preserve minimum data is also presented.

Keywords: Incident Response, e-Evidence Preservation, NTFS

1. はじめに

近年，情報化社会における，パソコンやスマートフォンなどの電子機器の発展が著しく，誰もが電子機器の利用が可能な時代になった．そのため，刑事・民事の裁判において，物的証拠だけではなく電磁的記録の証拠の重要性が増してきた．そこで，デジタル・フォレンジックの関心が高まってきている．

デジタルフォレンジックとは，インシデントレスポンス（コンピュータやネットワーク等の資源及び環境の不正使用，サービス妨害行為， データの破壊，意図しない情報の開示等，並びにそれらへ至るための行為（事象）等への対応）や法的紛争・訴訟に際し，電磁的記録の証拠保全及び調査・分析を行うとともに，電磁的記録の改竄・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術を言う．[2] 証拠の調査を行う場合は，対象物を直接調査・解析するのではなく，調査対象物と全く同じデータの複製を作成し，これを解析する．この際のデータ複製過程のことを証拠保全という．

パソコンやスマートフォンといった電子機器を使用し，犯罪が行われた場合，犯罪捜査を行うのには，警察をはじめとする司法機関が，これらの機器内のデータを電磁的証拠として集めることが必要となる．しかし警察内で証拠保全を適切に行える知識を持っている専門員や鑑識員は，捜査現場に行き渡るだけ十分に確保できるとは限らない．そのため，犯罪捜査の場において専門知識を持っていなくても使用できる，証拠保全ツールへの要求は高い．捜査現場においては，被疑者が事前に証拠の隠滅や隠蔽を行った可能性があるため，消去されたデータの復元や暗号化されたデータの解読，隠蔽されたデータの検出ができる技術も求められている．

[1] 立命館大学大学院情報理工学研究科
Graduate School of Information Science and Engineering, Ritsumeikan University
[2] 立命館大学情報理工学部
College of Information Science and Engineering, Ritsumeikan University

現在，警察の専門員や鑑識員は，犯罪に関連している機器のハードディスク (HDD) をはじめとした電磁記録媒体に対して，その全記憶領域を証拠保全している．実際には裁判において使用される電磁的証拠は記録媒体の容量に比して極めて小さいにもかかわらず，警察の専門員や鑑識員が，全記憶領域の証拠保全を行うのは，部分的に証拠保全を行った電磁的証拠は，その保全部分以外に被疑者に有利になるような証拠が存在していた可能性を被疑者や弁護人に指摘されることがありうるからである．そのような証拠の不存在を証明することは困難であるため，捜査現場では全記憶領域の証拠保全を行うのが原則とされている．

しかし近年では，記録媒体の容量が増加していることや一般に捜査対象となる電磁的証拠も膨大になってきたため，デジタル・フォレンジックに必要なデータの複製や解析にかかる時間が課題になってきた．そこで本論文では，全記憶領域の証拠保全を行う代わりに，必要最小限となる電磁的証拠のみが短時間で抽出可能であり，かつデジタルフォレンジックの知識を十分に持ち合わせていない現場の警察官でも使用できる，証拠保全ツールを提案し，それを試作した結果を報告する．

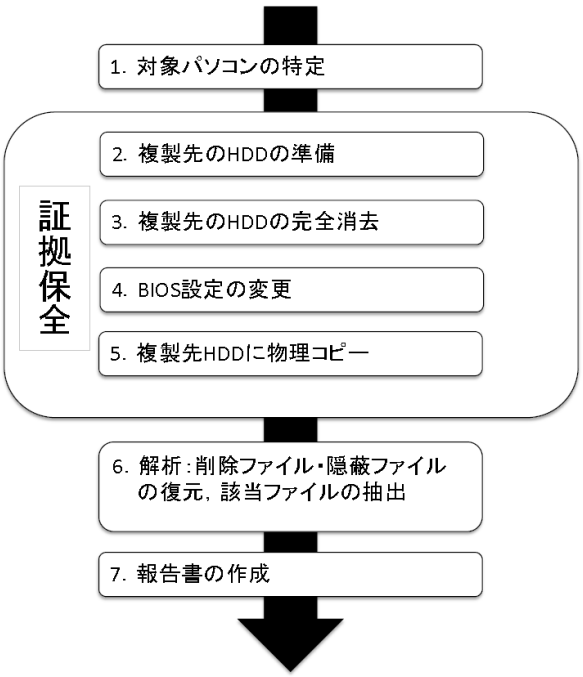

図 1　デジタルフォレンジックのプロセス

2. 研究背景

2.1 デジタルフォレンジックとは

現代社会の生活において，パソコンやスマートフォンなどの電子機器の利用が増加するにつれ，デジタル・フォレンジックへの関心が高まってきている．企業の業務において電子機器の果たす役割が大きくなるにつれて，そこで行われた作業において発生する法的紛争への対応の機会も増えている．業務上の不正や業務不履行，守秘義務違反による契約違反，内規違反などによる民事訴訟や，内部告発者保護法，e-文書法などが関連する民事訴訟または刑事訴訟への対応には，デジタル・フォレンジックが必要になってくる．企業内の情報システムにおいて，法的証拠となる電磁的記録の保全を正確に行い，改竄や削除がないことを後に説明できることは極めて重要である．

2.2 証拠保全の課題

デジタルフォレンジックでは，調査を行う対象物に記録されたデータを直接調査・解析するのではなく，調査対象物と全く同じ複製を作成し，複製したデータを解析の対象とする．これは調査や解析の過程でデータが改ざんされてしまうことを防ぐために極めて重要な手続きである．

図 1 は，デジタルフォレンジックの基本的な手順について説明している．ここでは，調査対象物を複製する際の過程を主に証拠保全と呼んでいる．一般に証拠保全は，電磁的証拠を複製する HDD 等のストレージの準備から始まる．証拠保全のための複製では，まず複製先の HDD は，あらかじめデータを完全消去した状態にしておかなければならない．これは，複製先の HDD に他のデータが残存していると，証拠の原本同一性が保証できないおそれがあるからである．また，証拠保全の対象となるパソコンは不用意に電源を入れると，通常，内蔵の HDD から起動される過程で一部のファイルのタイムスタンプが OS によって書き換えられ，証拠の改ざんがおきる．このため，証拠保全の前にはパソコンが内蔵用 HDD から起動せずに，外付けの記憶装置からフォレンジック用 OS を用いて対象パソコンを起動できるように BIOS 設定の変更を行う．HDD の複製では，対象のパソコンの内蔵 HDD を複製先 HDD に物理コピーを行う．ここまでが図 1 に示した証拠保全の一連の流れとなる．

近年のインシデント・レスポンスにおける証拠保全では，フォレンジック調査の対象物が増加していると言われる．対象物が増加している原因の一つとして考えられるのは，サイバー攻撃における「標的型攻撃メール」である．標的型攻撃メールは，攻撃者が組織内ネットワークへの侵入を行う目的で，特定の企業・組織を狙い，その組織にあわせたメール文面でマルウェアを送付する．このマルウェアによってパソコンの遠隔操作を可能にした後，攻撃者は組織内の多数のパソコンを同様に段階的に支配下に置こうとすることが多い．[11] 攻撃者が捕まり，捜査に至った場合，周囲の不特定多数のパソコンについても捜査の対象になる可能性が高い．そのため，フォレンジック調査を行わなければならない対象物が増加して証拠保全の長期化に繋がっていると考えられる．

2.3 HDD の容量推移

証拠保全で問題としてあがるのは，パソコン等の HDD や SSD の容量増加に伴う，証拠保全の実行時間である．HDD の 1 台あたりの記録密度は 2000 年以降は年 30〜50% で伸びてきており [3]，今後はその伸びは鈍化するものの年 20% 程度を維持すると見られている [4]．

これに対して HDD への読み書きの速度は十分に伸びていない．一般に，HDD の読み書きの速度はディスクの回転数と，メディア上の円周方向の記録密度に比例する．HDD のメディア回転速度は，3.5 インチメディアの場合，多くのドライブで毎分 5400 回転ないし 7200 回転から向上していない[*1]．記録密度は年々向上しているが，円周方向の線密度で言えば記録密度の二乗根でしか増加しないため，例えば HDD の容量が 2 倍に増しても書き込み速度は $\sqrt{2}$ 倍程度にしかならない．記録密度の向上はメディア枚数の追加でも行われるため，実際には転送速度の向上は $\sqrt{2}$ をやや下回る．結果として，HDD の容量が増加するとともに HDD の全記憶領域を証拠保全するにかかる時間は延び続けている．

2.4 証拠保全における物理コピーとは

証拠保全においては，HDD などの記憶媒体の中のデータを全て保全することが求められる．つまり，HDD 内に構築されたファイルシステムを全て複製し保全することが必要である．対象となるデータを複製する手法には，論理コピーと物理コピーの二つの方法がある．論理コピーはファイルそのものの複製や，ファイルシステムのメタデータの複製などの手法により HDD 内のファイルシステムをそのまま複製するものである．一方，物理コピーは HDD をセクタ単位で参照してその内容を全て複製するものである．これにより，ファイルシステムが現在ファイルを保存する領域として使用していない未使用領域を含めて複製が行われる．この未使用領域には，以前にデータが書き込まれていたが，該当するファイルが削除されたなどの理由でファイルシステムとしては空き領域になった部分が残されている．また，HDD のセクタは 512 バイトまたは 4096 バイトの固定長だが，ファイルの長さは任意のバイト数であるため，最後に使用されたセクタにはファイルの末尾の後ろに余剰部分が残る．これをスラック領域 (Slack space) と呼ぶ．未使用領域及びスラック領域には，過去に削除されたファイルや，故意に隠蔽されたファイルなどが，上書きされない限り残存している可能性がある．そのため，デジタルフォレンジックでは原則として証拠保全においては物理コピーを行う．その物理コピーには専用のソフトウェアまたはハードウェアが用いられるが，対象物に何らかの書き込みが行われ，証拠が損なわれることのないように，書き込み防止のための装置やソフトウェアが併用される．

[*1] 特に性能を求められる用途でのみ毎分 10000 から 15000 回転のメディアが使われている．

図 2　HDD:250GB の物理コピーの様子

表 1　物理コピーに使用した HDD

メーカー	容量	型番	使用用途
Seagate	250GB	VB0250EAVER	コピー元
Western Digital	500GB	WD5003ABYX	コピー先

図 2 に物理コピーの例を示す．この機器は，株式会社センチュリー製の「これ do 台 Hi-Speed（KD25/35HS）」である．この機器で実際に表 1 に示す 250GB の HDD を物理コピーした結果，1 時間 39 分 11 秒かかった．つまりこの製品での物理コピーの転送速度は，42.0MB/sec となった．これは，仮に転送速度が々だとすると 1TB の HDD の証拠保全は 6 時間，3TB の HDD の証拠保全は 18 時間程度かかる計算になる．このため，この証拠保全をいかに短い時間で実現するかが重要になる．

3. NTFS ファイルシステム

NTFS(NT File System) は現在の Windows で主に用いられているファイルシステムである．NTFS では，ファイルシステム内のすべてのデータは，メタデータを含めてファイルとして扱われている．[1]

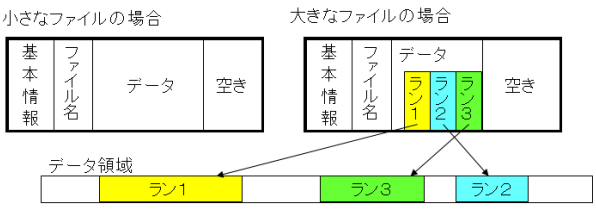

図 3　各 MFT エントリの構造

MFT(Master File Table) は NTFS のボリューム構造の中心であり，1kB ファイルレコードの配列として実装され，基本的には 1 個のファイルレコードが 1 つのファイルを表す．各ファイルレコードには 0 から順番に番号がついており，これが NTFS ファイル内の各ファイルに対する情報を保持している．なお，MFT 自身も$MFT という名前

のファイルであり，さらに$MFTmirr と呼ばれるファイルに複製されることによりバックアップされている．各ファイルに関する情報は，原則としていずれかの 1 つのファイルレコードから得られるが，ファイルの属性数が多い場合やファイルの断片化が進行している場合は，1 つのファイルに複数のファイルレコードが必要になる．MFT は属性情報により，ファイル名，ファイル属性，ファイル位置情報が記録されている．[1][6] MFT の属性情報は図 3 のように，十分に小さな場合はファイルレコード内に書かれ，これを常駐属性という．大きな属性は非常駐属性とよばれ，ファイルレコード内にはランと呼ばれる形式で，データ領域中のどの位置に書かれているかが示されている．各ランは先頭のクラスタ番号とクラスタ数で表現できる．ファイルがすべての連続したランに収められた時は，1 つのランの情報が収められるが，メディアのいくつかの部分に分散して収められたときは，そのランの数だけ情報が収められる．代表的な非常駐属性はファイルのデータそのものである．メディア内でファイルがあまりにも細分化され，データ部が多数のランに分割されたときは，1 つのファイルレコードには収まりきらなくなるため，$ATTRIBUTE_LIST と呼ばれる属性を用いて，複数のファイルレコードを連結して使用する．すなわち，このときは例外的に 1 つのファイルが複数のファイルレコードに対応することになる [6]．ファイルレコードの削除については，$MFT 内の各ファイルレコードが削除されているか否かを 1bit の情報の列で表現するビットマップと呼ばれるデータの値を変更して行われる．

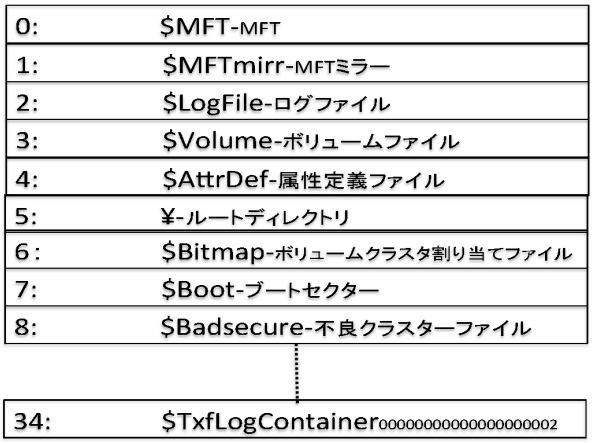

図 4　MFT の NTFS メタデータファイルのファイルレコード

このビットマップは，図 4 のようにファイルレコードの 0 番のファイルである，$MFT の$BITMAP 属性内で表現されている．また，クラスタを未使用状態に戻すには，ファイルレコード 6 番のファイル$Bitmap という別のビットマップで表現されている．[7]

Windows のファイルシステムである NTFS は，ボリュームの割り当て状態を$Bitmap ファイルに記述する．ビットマップファイルのデータ属性にはビットマップ自身も含まれており，各ビットはボリューム上のクラスターを表し，そのクラスターが空いているか，ファイルに割り当てられているかを示す [6]．

この他，Windows ではシステムの動作のため以下のようなファイルが使用される．Windows システムが休止状態に切り替わるときには，メモリの内容を圧縮して，hiberfil.sys という休止状態ファイルに保存する [6]．このファイル内にはその時点でのメモリの内容が保持されている．pagefile.sys ファイル (スワップファイル) は，仮想記憶のために使用されるファイルである．つまり pagefile.sys ファイルには，ワークセットが主記憶容量を超えた時点で，使用していないメモリ領域の内容が追い出されて書き込まれている [1]．Temp file(テンポラリファイル) は，ソフトウェアが，作業中のデータの保存のために一時的に作るファイルである．アプリケーションによっては処理中のデータの一部を書き込んでいる．Prefetch file(プリフェッチファイル) には，Windows 起動時に真っ先に使用するプログラムや，その後頻繁に起動するプログラムが記録されている．Windows は，この情報を複数の小さなファイルとしてプリフェッチフォルダに保存する．次に再びパソコンの電源を入れるとき，Windows はこれらのファイルを参照し，起動プロセスを高速化するのに役立てている．レジストリとはデバイスドライバ情報，アプリケーション設定，ウィンドウズ設定，パスワード，Windows PC 上の全ての設定を格納する階層型データベースである．レジストリファイルはこのレジストリのデータを保持するファイルである．

4. 関連研究

本研究の関連研究または類似研究として挙げられるものは，以下の通りである．

白石らは，保全データの優先順位付けと証拠保全の際に原本同一性を保証するためのヒステリシス署名を用いて携帯端末に対する証拠保全についての提案，及び携帯端末系統インシデントの証明とユーザ自身の振る舞いを研究している．[8] 白石らは，原本同一性を携帯端末で保証する際，ヒステリシス署名を用いる．しかし，ヒステリシス署名は, その連鎖を辿ることでファイルを改変される問題がある．この問題への対処として, セキュリティデバイスを用いる方式が提案されている．この方式では, 連鎖用のデータとしてファイルではなく, セキュリティデバイス内の耐タンパ領域にある情報を用いる．これにより, ヒステリシス署名の問題へ対処している．[13] そのため，タイムスタンプ方式の方が署名の連鎖が少ないため，ファイル改変がおきにくいと考えられる．

小川らは，システムで書き込もうとした内容の履歴を時刻とともにすべて保管し, 分析時に任意の時刻の状態で

データを再現するものを行っている．提案システムは仮想計算機モニタを利用しているためゲスト OS が攻撃を受けても継続して動作することで, ホスト OS に保存された保全データの改竄を防ぐことができるシステムである．[9] 小川らの提案は逐次，内容履歴をすべて保管するものだが，すべてのデータを保存していては効率が悪い．

Mehrotra, T. らは，python ベースのツールを作成して，イメージメタデータの解析と Windows7 の削除されたものを復活させることができる．Mehrotra, T. らが作成したツールが windows7 のみの対応で今後 OS 変更に対応できない点が問題がある．[10]

5. 提案と実装

5.1 研究の目標

本研究では，デジタルフォレンジックにおける証拠保全の時間を短縮するため，NTFS および Windows の動作を吟味した上で，できるだけ少ないデータによる証拠保全を目指す．具体的には，削除ファイルの復活後にスラック領域の調査によって新たな証拠が発見されることがまれであることから，ファイルのメタデータと重要なファイルの保存により証拠保全を行い，物理コピーを回避する．この際，デジタル・フォレンジックについての知識を十分に持ち合わせていない人物でも証拠保全を行うことが可能にする証拠保全ツールの作成を目指す．

6. 部分的証拠保全

部分的な証拠保全を行うにあたって，Windows 内のファイルのどの部分を保全するべきか検討した結果は表 2 通りである．

表 2 部分的証拠保全箇所

部分的証拠保全箇所	内容
$MFT	メタデータの格納域と データ本体の配置情報
$Bitmap	ファイル削除時の両方の空き領域の管理
hiberfil.sys	Windows が休止状態に移る前に 必要なデータを一時保存して おくためのファイル
pagefile.sys	物理メモリの空きがない際に データの一時退避に使用
Temp フォルダ	編集中ファイルなどの一時ファイル
Prefetch	頻繁に起動するプログラムの記録
Registry	アプリケーションの設定内容等
個人のファイル	.word や.txt など個人のもの

表 2 において個人ファイルとは通常の Windows のインストール設定に置いてはシステムデイスクの Users(ユーザ) フォルダ以下に入っているデータである．ここが最も大きなデータとなる．

以下，各項目について証拠保全の対象とした理由を述べる．

6.1 $MFT

MFT は当該 HDD 内の全てのファイルの名称や作成日時，アクセス権，ディスク上の位置情報を保持している．ファイルが数百バイト程度に小さい場合には，ファイルレコード内にデータが保持されている．ファイルのデータが複数のクラスタに渡り格納されている場合は，位置情報は MFT 内にある．ファイルが既に削除された場合であっても，これらの属性情報は MFT 内に残存しているため，そのデータを保持していたクラスタが上書きされない限り，データはディスク上に残存している．よってこの属性情報を利用して，削除ファイルを復元することもできる．

6.2 $Bitmap

$Bitmap はデータ領域を表しており，クラスタの利用状況を管理する．削除ファイルについてそのクラスタが使用されていることがわかれば削除ファイルの復活は困難であることが容易に分かるため，その処理を省略することができる．

6.3 hiberfil.sys

このファイルには Windows を休止状態にした時点での主記憶内容が全て保存されるため，これをフォレンジック調査することで，その時点でどのようなプログラムやプロセスが動作していたということや各プロセスがどのようなデータ情報を持っていたのか知ることができる．また，アプリケーションにより文書ファイルが暗号化されていた場合でも，そのプログラムが当該ファイルにアクセスしている状態で休止状態になっていた場合，その内容が読み取れる可能性がある．

6.4 pagefile.sys

このファイルは仮想メモリ内のデータの一部が書き込まれているため，hiberfil.sys と同様に証拠となる情報を取り出すことができる可能性がある．

6.5 Temp フォルダ

Temp フォルダには，対象となる犯罪や不正に使用されたアプリケーションなどの一時ファイルが存在している場合があるため，これを証拠として分析に役立てられる可能性がある．

6.6 Prefetch

Prefetch ファイルを調査することで，Windows 利用時に頻繁に使用されていたアプリケーションの実行ファイルのパス，最後に実行された日時や回数，関連するファイルパスなどを確認することが可能である．これにより，そのパソコン上で何が行われていたか推測できる．

6.7 Registry

Regidtry は，各アプリケーションの設定状況が把握できるほか，調査対象のパソコンにおける外部接続機器 (USB メモリーや SD カード，外付け HDD 等) の接続履歴を調査し，それらの機器にファイルがコピーされ持ち出された痕跡がないか調査を行うために使用できる．また，アプリケーションによって頻繁に用いられたデータファイルについてもそのパス名と最終アクセス日時がわかるため，電磁的証拠として利用可能な多くの情報を含んでいる．

6.8 個人ファイル

個人ファイルには，当該パソコン上で行われていた作業や活動に関する多くの情報が含まれている．しかし場合によってはその量が膨大となり証拠保全の時間短縮に繋がらない可能性があるため，場合によってはファイルの更新日時やアクセス日時を元に，利用頻度が高いもしくは犯罪や不正行為の直前に使用した可能性が高いファイルを優先的に証拠保全することもできる．その場合であっても，$MFT を保存しておくことで，ファイル名や日時など属性情報だけは全て保全できる．

7. 実装

7.1 実装環境

証拠保全ツールの試作にあたっては，容量 128GB の USB フラッシュメモリを使用した．これに比較的軽量な Linux として知られる Puppy Linux Precies-571JP[12] を導入し，以下のようなスクリプトを実装してツールとした．Linux は NTFS パーティションの読み取り機能を持つため，このようなツールの実装に適している．

7.2 起動時スクリプト

本証拠保全ツールでは，証拠保全の対象となるパソコンにこのツールが導入された USB メモリを装着してこれから起動し，適切なスクリプトを実行することによって HDD 内の電磁的証拠を USB に転送する．起動時スクリプトは，USB による Puppy Linux 起動時に実行される．起動にあたっては PC 内のドライブを操作した上で NTFS パーティションを探し，読み取り専用で mount することで，証拠保全の際，HDD の内容に変更を加えられていないことを保証する．これにより，当該 USB メモリから起動した際にすべての HDD 等の電磁記録媒体が，読み取り専用で mount されるようになる．

8. 証拠保全実行スクリプトについて

証拠保全実行スクリプトは，証拠保全の対象とするファイルを USB メモリ内に複製するものである．本ツールでは，実際の証拠保全前に削除ファイルの復活や他の簡易調査を行う可能性を考えて，起動時に自動的に証拠保全が行われるしようとはしていない．本ツールでは，「triage_copy」というファイル名で証拠保全実行スクリプトを作成した．これの実行により，6 節で述べたファイルが USB 内に取り込まれる．個人ファイルについてはすべて証拠保全すると USB メモリ内に入りきらない可能性があるため，設定では更新日時が早い順に並べ替えて，USB メモリ内に収まりきらなくなるまで複製を続ける仕様とした．

9. 本証拠保全ツールの使用方法

本研究で試作した証拠保全ツールの使用方法は以下の通りである．

事前準備：BIOS 設定で OS 起動順序を USB 優先起動に切り替えておく

-実行順序-

1. 保全対象の機器に USB を取り付ける．
2. 電源を入れると OS 選択画面で Puppy Linux を選択する．
3. 起動時スクリプトが実行される．
   読み取り専用 (Read Only) で PuppyLinux が起動する．
4. デスクトップ画面が表示される．
   コマンドプロンプト (端末) をダブルクリック．
5. コマンドプロンプトに「triage_copy」というコマンドを入力
   Enter キーを押す (コピーが実行される)
6. デスクトップ上の「ファイル」アイコンをダブルクリックで開く
7. コピーの確認をするため USB メモリ内の my-documents/sd_copy の中を確認する．
8. パソコンのシャットダウンを行う．

以上の順序でコピーは完了する．「triage_copy」コマンドを実行した際，保全中のファイル名とそのタイムスタンプが表示される．この内容と経過時間によっては，保全の作業を中断することもできる．

10. 実験成果

今回作成した証拠保全ツールとこれ do 台 Hi-Speed（KD25/35HS）という完全コピーを行う製品で証拠保全のスピードを比較したグラフが図 5 である．今回は，250GB の Seagate 製 HDD を使用して実験を行った．

図 5 証拠保全時間の比較グラフ

図 5 の上段のグラフである「ツール使用時」は，今回作成した，証拠保全ツールを使用した時の結果である．証拠

保全ツールを使用して，部分的な証拠保全を行った場合，12 分 4 秒で証拠保全が終了した．一方，「高速完全コピーツール使用時」は，1 時間 39 分 11 秒，証拠保全に時間が必要としている．このように今回試作した証拠保全ツールが，この実験環境では約 8 倍動くことが確認できた．そのため，証拠保全の時間短縮という目標は達成できた．しかし課題も残った．今回の実験環境では個人ファイルの量は 4GB 弱であったため，証拠保全されたデータ量は 4.6GB ほどに過ぎない．これは物理コピー時の 20 分の 1 以下のデータ量であるが，それにもかかわらずこの程度の速度になるのは，Linux の NTFS ファイルシステムの実装の問題により，ファイルの読み出し速度がそれほど高速でないことに起因すると考えられる．

11. まとめと今後の課題

本研究では，デジタル・フォレンジックにおける証拠保全の時間短縮を目指し，Windows において最小のデータ量によって証拠保全を行う方法を検討し，その実装を行った．簡易な実装ではあるが，時間短縮効果については個人ファイルのデータ量が少ない場合には十分に得られることを確認できた．

今後の課題としてあげられるものは大きく分けて二つある．一つ目に原本同一性の保証を行うためのタイムスタンプ電子署名の実装である．コピー元の原本と同一であることを証明するため，電子データにタイムスタンプを付与することで，今ここに確実に存在していたという「存在時刻」とタイムスタンプ付与時の状態である，「完全性」が証明することができる．そのため，証拠保全ツールでコピーを行うと同時にタイムスタンプ電子署名という形で原本同一性の保証を行うことが今後の課題の一つである．二つ目に，今回は見送った削除済みファイルの復元である．NTFS のファイル復活そのものは，該当のデータ領域が上書きされていない場合にはそれほど困難ではないため，早急に実装したい．

また，Linux による実装に性能問題があることが分かったため，USB から昨日可能な Windows である WinPE による実装も検討している．さらに，本当にデジタル・フォレンジックの知識を持たない使用者に対応するために，ユーザインターフェースの改良なども課題としてあげられる．

参考文献

[1] 佐々木良一，舟橋信，安冨潔ほか：改訂版 デジタルフォレンジック事典，日科技連，2014.

[2] 特定非営利活動法人デジタル・フォレンジック研究会：デジタルフォレンジックとは，入手先 ⟨h⟩ttps://digitalforensic.jp/home/what-df/.

[3] 服部 正勝, 鈴木 博, 菅谷 誠一：HDD, ODD 及び SSD の技術動向, 東芝レビュー Vol.66, No.8, pp.30–35, 2011.

[4] 福田 昭：HDD 世界出荷台数は過去 6 年で約 3 分の 2 に減少，インプレス社 PC Watch，入手先 ⟨h⟩ttp://pc.watch.impress.co.jp/docs/column/semicon/1045367.htm 2017.

[5] Mark E Russinovich,David A. Solomon,Alex lonescu：インサイド Windows 第 6 版 上, , 日経 BP 社, 2012.

[6] Mark E Russinovich,David A. Solomon,Alex lonescu：インサイド Windows 第 6 版 下, 日経 BP 社, 2012.

[7] 特定非営利活動法人デジタル・フォレンジック研究会 「証拠保全ガイドライン 第 6 版」, 入手先 ⟨h⟩ttp://www.digitalforensic.jp/eximgs/20130930gijutsu.pdf.

[8] 白石 陽, 三科 貴, 高橋 修：フォレンジック技術を利用した携帯端末のための証拠保全手法, 情報処理学会論文誌, Vol.54, No.1, pp.91–102, 2013.

[9] 小川 拡, 平野 学：仮想計算機モニタを利用したコンピュータフォレンジックスのための補助記憶装置のデータの保全と回復のシステム, 情報処理学会技術報告, 2013-CSEC-60, Vol. 16, pp.1–8, 2013.

[10] Mehrotra, T. and Mehtre, B.M., *An automated forensic tool for image metadata and Windows 7 Recycle Bin*, 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014.

[11] 情報処理推進機構:『高度標的型攻撃』対策に向けたシステム設計ガイド, 入手先 ⟨h⟩ttps://www.ipa.go.jp/security/vuln/newattack.html, 2014.

[12] Puppy Linux 日本語版 入手先 ⟨h⟩ttp://openlab.jp/puppylinux/.

[13] ログ保全と攻撃難化によるセキュリティ向上技術に関する研究 著者:佐藤 将也 岡山大学大学院自然科学研究科

http://ousar.lib.okayama-u.ac.jp/file/52978/K0005044_fulltext.pdf