1Z-10

時間経過に着目したHDDのデータ復元実験とその評価

木田敦隆† 佐々木良一†

東京電機大学†

1 はじめに

近年，高度情報化社会の進展に伴い，企業で個人情報を取り扱う機会が増え情報漏えいや消失等の事故を起こしてしまうリスクが問題になっている．日本情報経済社会推進協会の調査によると，個人情報を誤消去してしまう事故が平成23年度には17件，平成24年度には21件報告されている[1]．多くの企業で事業がIT化されている今日，意図せずにPCの重要なデータを削除してしまう脅威は常に存在している．

デジタルデータの保全・復元具技術であるデジタルフォレンジック技術[2]を利用した復元ソフトを用いることにより，誤って削除してしまったデータも復元可能であるが元の領域に上書きされた場合は復元できない．そして，PCの環境や削除後の作業によって復元率復元率が時間とともにどのように変化するかについては明らかにされてこなかった．

本研究ではこれらのことを明らかにするために，複数の環境において様々なPCの使用方法でデータの復元実験を行いその復元率にどの様な差が生まれるのか考察した．

2 実験内容

2．1 実験概要

PCの環境や，PCで行う作業によって復元率にどのように差が生まれるのかを検証するために3つの実験を行った．

2．1．1 実験１概要

内蔵HDDのCドライブ領域に実験用フォルダを作成し，実際に実験用のファイルを作成・保存する．実験用ファイルがHDDに書き込まれたのを確認した後そのファイルを削除する．その後実験用ファイルが保存されていたクラスタが他のファイルによって上書きされる時間及び上書きしたファイルを調べた．実験1では，ファイルを削除した後PCでは一切の作業をせず電源をつけたまま放置した場合について調べた．

2．1．2 実験２概要

基本的な手順は実験1と同様だが， 実験2ではファイルを削除した後1時間ごとに新しく削除したものと同じ1MBの画像ファイル(jpg)を実験用フォルダに10個作成・保存した場合と， 1時間ごとに新しく10MBの画像ファイル(jpg)を実験用フォルダに10個作成・保存した場合について調べた．

2．1．3 実験３概要

基本的な手順は実験1，実験2と同様だが，実験3では，ファイルを削除した後PCを普段通りに使用した場合について調べた．ここでいう普段通りとは，実験中のPCの使用者が実験中ということを意識せずにPCを使うことを指す．

2．2 実験環境

実験1，実験2は表1の環境で行った．

2．2 実験環境

実験1，実験2は表1の環境で行った．

表１．実験１，実験２のOS環境

OS	Memory	CPU	HDD容量
Windows7	16.00GB	Intel Core i7	160GB

実験3は研究室のメンバー6人で行った．また実験時のそれぞれの環境をA～Fとして表2に表記する．

表２．実験３のOS環境

	OS	Memory	CPU	HDD容量
A	Windows7	16.00GB	Intel Core i7	160GB
B	Windows7	8.00GB	Intel Core i7	500GB
C	Windows7	4.00GB	Intel Core i5	250GB
D	Windows7	2.00GB	Intel Celeron	200GB
E	Windows7	4.00GB	Intel Core i5	250GB
F	Windows7	4.00GB	Intel Core i7	500GB(SSD)

それぞれの実験に用いる削除用ファイルとしては，1MBの画像ファイル(jpg)を用いた．また，復元ソフトはForensic tool kitを用いた．

2．3 実験方法

各実験の手順を以下に示す．

2．3．1 実験１

(i) 削除する実験用ファイルをCドライブ・マイドキュメント上の実験用フォルダに用意する
(ii) ファイルの中身と保存されたクラスタを確認し，保存したファイルを削除する(shift + del)
(iii) ファイルを削除後，PCでは一切の作業を行わず1時間ごとにファイルが保存されていたクラスタを調べる
(iv) ファイルが上書きされていたら，上書きされた時間，上書きされたファイルを確認する

2．3．2 実験２

手順(i)，(ii)，(iii)は実験1と同様である
(iv) ファイルが上書きされていたら，上書きされた時間，上書きされたファイルを確認する

2．3．3 実験３

手順(i)，(ii)，(iii)は実験1と同様である
(iv) ファイルが上書きされていたら，上書きされた時間，上書きされたファイル，行っていた作業を確認する

"Experiments and Considerations of Data Restoration of HDD Focused on the Passage of Time"
Atsutaka Kida†, Ryoichi Sasaki†
Tokyo Denki University†

3　実験結果

3. 1　実験１結果

図1に実験1の結果を示す．実験1は15回行い，その復元率をグラフにまとめた．

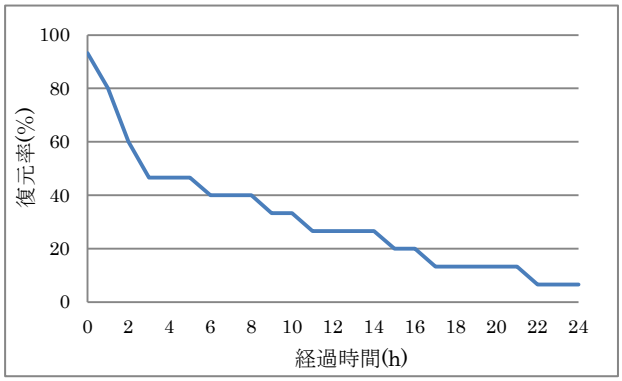

図１．実験１結果

3. 2　実験２結果

図2に実験2の結果を示す．実験2は15回行い，その復元率をグラフにまとめた．①が1MBの場合，②が10MBの場合である．

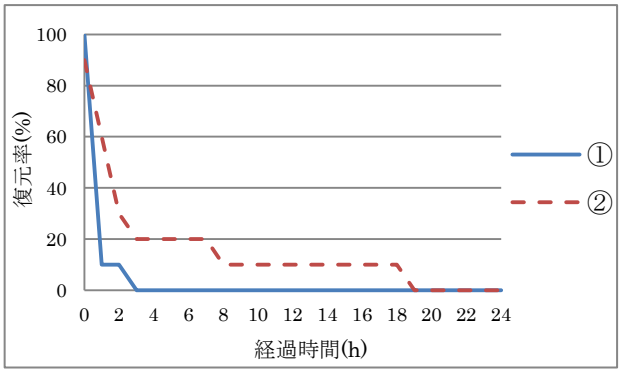

図２．実験２結果

3. 3　実験３結果

以下に実験3の結果を示す．実験3はAでは15回行い，その他のPCでは10回ずつ実験を行った．その復元率をグラフにまとめた．

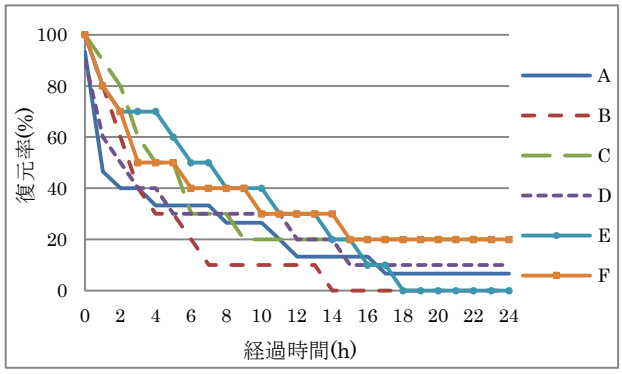

図３．実験３結果

4　考察

4. 1　実験１考察

実験1とその他の実験のグラフを比べると，一定時間ごとに新しいファイルを作成･保存した場合や普段通りに使用した場合，PCを放置した場合に比べて復元が不可能になる時間が短いということがわかる．

4. 2　実験２考察

10MBの画像ファイルを作成・保存した場合に比べて，1MBの画像ファイルを作成・保存した場合の方が復元できなくなる時間が早いことがわかる．また，1MBの画像を作成･保存する実験の場合は該当のクラスタに新しい画像ファイルが書き込まれることが多かった(5/10回)が，10MBの画像を作成・保存した場合はすべてその他のファイルで上書きされた．この結果に関しては，NTFSにおいて断片化を避けるアルゴリズムが影響していると考えられる．

4. 3　実験３考察

各環境での結果を比較した結果，インターネットブラウザとしてGoogle Chromeを使用している場合ではキャッシュが多いということが分かった． Internet Explorerの場合も，一時ファイルが多く書き込まれた．また，VMを使用している環境ではVirtualMachineのスナップショットが多く書き込まれていることを確認した.その他はソフトウェアやプログラムのアップデート，Windowsのプリフェッチが大半だった．Fの環境において，SSDの環境でも実験を行ったがHDDの環境との明確な差は見られなかった．

4. 4　全体の考察

各実験の結果から，Cドライブを用いた場合はファイルを削除してから24時間後には大半が復元できなくなることがわかった．また，クラスタによっては上書きされるまで時間がかかり，中には24時間以降も復元できるファイルが存在した．このことから，大事なデータは書き込み頻度の少ないDドライブや，外付けのストレージに保存することが重要であることがわかる．

5　まとめ

本稿ではデータの削除後，データが復元できなくなる時間やその原因を明らかにするために実験を行い，それを評価した．HDDに対する書き込み頻度が高い作業をするほどファイルが復元できなくなる時間が早まることがわかった．このことから，重要なデータはDドライブや外付けHDDなど，HDDに対する書き込み頻度が少ないストレージに保存することが重要であるということがわかった．

また，本研究の今後の方針としては，

(i) 各実験の試行回数を増やすとともに，実験中のPCの作業にバリエーションを持たせる

(ii) PCのスペックに差を設ける

(iii) HDDの空き容量によって復元できなくなる時間に差が生まれるのかを調べる

などが挙げられる．

参考文献

[1]「個人情報の取り扱いにおける事故報告にみる傾向と注意点」について(2013．7)
http://privacymark．jp/news/2013/0712/index．html

[2]フリーソフトによるデータ抹消・復元大全(2013．1)
http://www．cybernetic-survival．net/w_s．htm