消去アクセス難易度別にみるHDDのデータ領域３分類

～　論理セクタ・代替処理後の不良セクタ・PARADAIS　～

大阪データ復旧（株）　下垣内 太

１．磁気ディスク上における論理セクタの位置はHDDの制御機構に依存

HDD内部には、データが記録される円盤状の磁気ディスクがあり、回転する磁気ディスク上をスイングアームが水平方向に移動しスイングアームの先端にある磁気ヘッドが磁気ディスク上のトラックを追従してセクタ毎にデータを読み書きする仕組みになっています。


図１．データアクセス時

また、各セクタには論理アドレス番号（LBA）が割り当てられており、ユーザは磁気ディスクにおけるセクタの物理的な位置を意識することなくLBA指定することで読み書きの対象となるセクタ情報へアクセスすることができます。

そしてNTFSなどのファイルシステムを用いることでユーザは論理アドレス番号を意識することなくフォルダやファイルを指定することで読み書きの対象となるデータにアクセスすることができます。

このように、パソコンユーザがファイルにアクセスする際には、まずファイルシステムの構造情報を基にアクセス先データの記録位置が論理アドレス番号でHDDに指定され、次にHDDは指定された論理アドレス番号に基づいて物理的なセクタ位置を指定し、そして磁気ヘッドがその位置まで移動してからデータの読み書きが行われます。


図２．電源OFF時

このことは、HDDの複製装置やイメージ取得ソフトウェアを用いて行う証拠保全の際も同様であり、最初の論理ブロックから最後の論理ブロックまでを連続して読み出す際にも、保全用ツールからはデータ取得対象セクタを論理アドレス番号で指定され、HDD内部ではその指定された論理アドレス番号を物理的なセクタ位置番号に変換しながらデータ読み出し要求に応えています。

以降、論理アドレス番号をLBA（Logical Block Address）と表記し物理的なセクタ位置番号をPBA（Physical Block Address）とします。また、本書では１セクタは512バイトの仕様を前提に書かれておりますが、１セクタ4K仕様の製品においても基本的な構造は同じです。

２．HDDのデータが保存される領域は物理的にみれば流動的

HDDには、LBAとPBAを相互変換する機能が備わっており、この機能の実行に必要となる情報は磁気ディスク上のサービスエリア（システムエリア、以下SAと省略）と呼ばれる領域にファームウェアの一部として記録されています。そして、HDDの製造過程においては磁気ディスク上のセクタ数は製品

仕様上の全セクタ数（LBA数と同じ）よりも多く確保されており、出荷前に実施される性能検査工程を経てLBAを割り当てるセクタとそうでないセクタに分類され、前者セクタ領域についてはユーザがデータアクセス可能な領域となるようLBAが割り当てられます。

	HDD-1	HDD-2	HDD-3
全ＰＢＡ数	3,933,712,984	3,933,659,976	3,931,988,368
差（sectors）	26,683,816	26,630,808	24,959,200
差（Bytes）	13,662,113,792	13,634,973,696	12,779,110,400
差（%）	0.678%	0.677%	0.635%

図３．同型製品３台（2TB / LBA:3,907,029,168）のPBA数及びLBA数との差を調査した結果比較表

※第11期デジタル・フォレンジック研究会総会時講演会『保全性の高いデータ復旧技法（HiDR）とディザスタデータリカバリ』（2014年5月13日）での発表資料より抜粋

このような製品の成り立ちも踏まえますとHDDのデータアクセス時における磁気ディスク上のセクタ位置決定の仕様はファームウェアの機能に依存しており、工場で製造された全てのセクタにユーザがアクセスできる製品構造ではないこともわかります。

また、HDDには製品としての性能を維持する機能として不良セクタの代替処理機能が備わっています。LBAが予め割り当てられ、ユーザからのアクセス要求に応えてきたセクタへの書き込み性能が低下、ないし不能と判断された際に、HDD内部でそれまでLBAが割り当てられていなかった予備のセクタにLBAを発行しなおす機能です。

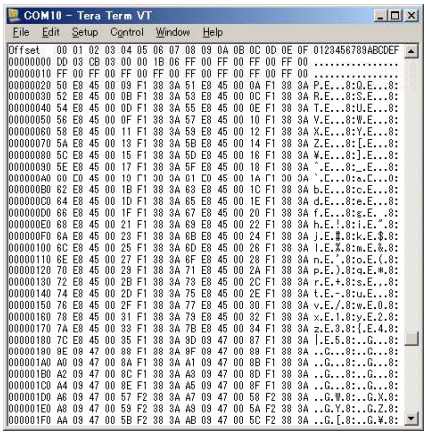

図４．シリアルコンソールによるセクタ代替処理機能ファームウェアのバイナリ表示 ※一部

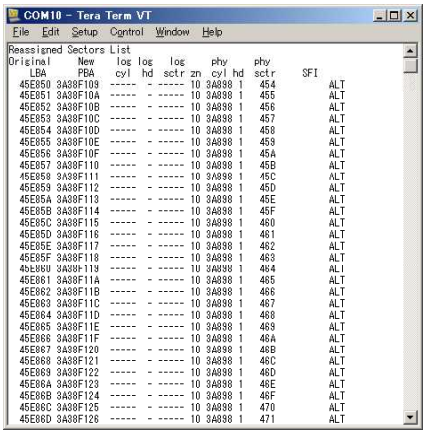

図５．可視化されたセクタ代替処理レコード
※図４と内容は同一

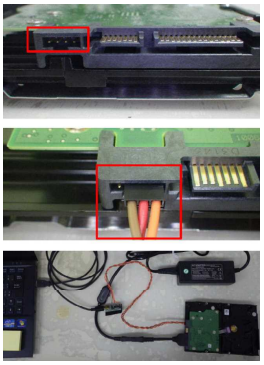

図６．シリアル端子（上）をUSBシリアル変換ケーブル（中）でPCと接続（下）し、セクタの代替処理状況を確認できる製品もある

これらのことからHDDの動作仕様として、ユーザがアクセスできる領域は製造者の決定するファームウェアによって管理されており、不良セクタ代替処理の発生前後ではデータが記録されているセクタの物理的な位置が異なるものであるため、製品出荷時の状態が必ずしも持続するものではなく、使用時間が経過するにつれてデータ記録位置が変動する性質を機能として有する情報記憶媒体であることがわかります。

３．代替処理後の不良セクタのデータ消去はEnhanced Secure Eraseに依存

性能不十分と判定された不良セクタはLBAの割り当て対象外になるため、ユーザはその後アクセスすることができません。そのためユーザはそのセクタに記録されている情報を読むことができません。また、データ消去とは、元々記録されていた情報とは異なる情報を書き込むことによって元々記録されていたデータを消失させることですが、LBAが割り当てられていないセクタにはユーザは何も書き込むことができません。

いかにデータ消去ソフトウェアを用いて消去回数を増やそうとも、LBAの割り当てられていないセクタへのアクセスは不可能ですので、たとえ35回の消去処理を実行したとしてもソフトウェアの消去処理対象にはならないセクタに記録されている情報として消去されることなく残り続けることでしょう。

しかし、HDDのファームウェアにはそれら不良セクタの代替処理の実施に関する記録機能があり、HDD自身に備わったデータ消去機能であるEnhanced Secure Eraseが正常に実装されている製品においては、代替処理された不良セクタの磁気ディスク上における物理的位置の特定およびアクセスが可能であるため、データ消去処理の対象とすることができます。

図７．Enhanced Secure Erase がサポートされていることの表示

このようにHDD内部の磁気ディスク上のセクタへのアクセスは全てファームウェアに管理されていますので、ユーザがアクセスできるセクタはLBAの割り当てられている領域のみに限られおり、またEnhanced Secure EraseはATAコマンドであるため、HDD内部で機能しLBAの割り当てを失った不良セクタ迄を消去対象に含むことができますが製造者の作成したファームウェアによる管理を超えることはできません。


図８．HDDEraseV4.0実行状況

消去処理対象のセクタ数が、製品容量セクタ数を上回ることができうる唯一のデータ消去機能が、ATAコマンドを利用したEnhanced Secure Eraseであり、現時点に於いてデータを消去できる範囲が最も多いデータ消去方法です。

４．Enhanced Secure Eraseでも消去が及ばないデータ領域 ”PARADAIS”

Enhanced Secure Eraseを実施してもなおデータが潜み続ける領域がHDDに存在することがこれまでの研究により分かりつつあります。その領域に記録されたデータはHDDをフォーマットをしても残り続け、ＯＳをインストールしても存在し続け、そこにマルウェアが存在しても駆除用情報セキュリティシステムでは検出することができませんので、その領域は、いわば誰の手も及ばない無法地帯であるとも言えます。その領域のことを当研究を進めるにあたり”パラダイス（以下、PARADAIS）”と呼んでいます。

このPARADAISがどのメーカーのどの製品にどの程度存在しうるのかについては、まだ調査の余地が

残されていますが、少なくとも現時点において既に存在そのものは確認できており、本書執筆時点（2016年3月26日）迄に計8回の講演や勉強会にて、のべ200名を超えるデジタル・フォレンジックス及びサイバーセキュリティの専門家の方々への解説と、デモの際にはEnhanced Secure Erase実施後のHDDからWindowsXP OSが起動したり、Debian GNU/Linux のrootパスワードすげ替えの様子をご確認いただいております。

また挙動面において、PARADAIS発動のタイミングは外発的なコマンド制御によるものと、内発的なトリガーによるものとの両方があり、特に後者の場合においてはオフラインのスタンドアロン状況でも自発的に発動しうるものですので、インターネットにつながっていないインフラ系システムがサイバー攻撃の標的となりうる危険性とも関連が出てきます。

このように、従来のデータ消去手法では消し去ることができず、事前検知や事後検証が非常に困難ないし不可能なデータ領域が存在することは、カスペルスキー社が昨年発表したファームウェア領域に存在するマルウェア等のような、サイバーセキュリティに絡まなければ考慮する必要がないとも考えることはできますが、証拠保全先HDDの取り扱い面においては、少なくとも不要データの存在は避けることが適切であり、このためにも代替処理された領域はデータ消去処理の対象に含めることが必要であり、この点については Enhanced Secure Erase機能によるデータ消去処理は、その動作が期待どおりに実施される場合においては有効であると考えられます。

５．おわりに

ＨＤＤやＳＳＤはメーカごとの設計によって構造が異なるため、本書に記載されている事項についてはより具体的かつ正確性を確保するためには、各製品の設計や仕様に沿った検証が本来ならば必要です。しかしながらそれらの情報は、ともすれば特定のメーカや製品の信頼性に影響を及ぼし兼ねない、との考えにより、特定のメーカ名や製品名を含め積極的に公表することは本書内では控えております。

また、この文書には実施することでデータや製品に不具合の生じる可能性がある技術的内容が含まれています。記載の目的は、消去アクセス難易度別にみるHDDのデータ領域３分類の解説のためであり、実証実験の実施等を奨励するものではございません。いかなる損害やトラブルが生じましても、当方は一切責任を負いかねますので予めご了承ください。

以上