Vol.2015-CSEC-71 No.12
2015/12/4

SSD の Over Provisioned Capacity からのデータ抽出手法

前田　恭幸[†1]　湯淺　墾道[†2]

概要：近年，スマートフォンを始め，パーソナルコンピュータ，タブレット端末，多機能周辺機器などに使用される不揮発性記録媒体のひとつであるフラッシュメモリの普及が急激に広がっている．不揮発性記録媒体のフラッシュメモリを搭載している SSD（Solid State Drive）を調査してみると，SSD 市場の 2017 年までの平均成長率は 39．2%と IT 調査会社 IDC は予測している．SSD には書換え寿命などの対策のため，Spare Capacity 及び Over Provisioned Capacity という予備のデータ保存領域がある．通常の方法ではデータにアクセスすることができないこの領域からデータ復元できたとする報告もある．また，SSD は HDD に比べ，データの記録構造などが異なるためデータの完全復元がしにくいと言われている．デジタル・フォレンジックの観点から，HDD と SSD のデータ復元の違いについて述べる．そして，SSD の Over Provisioned Capacity からの新たなデータ抽出手法を提案する．

キーワード：SSD，デジタル・フォレンジック，Over Provisioned Capacity

Data extraction method from the SSD of Over Provisioned Capacity

MAEDA YASUYUKI[†1]　YUASA HARUMICHI[†2]

Abstract:In recent years，the SSD market is growing rapidly．As the countermeasure to the problems such as the rewriting life to SSD，there is a spare data storage area of the spare capacity/area and Over Provisioned Capacity． Also it was reported that they can recover the data that can not be accessed from the areas in the usual way． SSD is also the conclusion that it is difficult to complete restoration of data compared to HDD． From the point of view of digital forensics， We consider the differences in data restoration of HDD and that in SSD． Then，we propose a new method of data extraction from Over Provisioned Capacity of SSD.

Keywords: SSD，Digital Forensic，Over Provisioned Capacity

1. はじめに

近年, パーソナルコンピュータにおいて SSD の利用が増加している. ノート型のパーソナルコンピュータなどにも，SSD が多く見られるようになった. IT 調査会社の IDC japan によると，SSD などフラッシュ技術を利用したストレージの 2013 年の売上額は前年比 75．4%増の 112 億円が見込まれており，SSD 市場の 2017 年までの平均成長率は 39．2%と予測されている．a

ノートパーソナルコンピュータなどにも SSD が多く見られるようになった．HDD と SSD を比較すると，読込み速度（一例として，ベンチマークで，HDD:WD20EARX と SSD:ADT S510 AS510S3 を比較すると，読込み速度・書込み速度はともに約 3 倍，ランダムアクセスは約 40 倍），軽さ, 電力消費量などの面で SSD のメリットは魅力的である. HDD のメリットは, SSD に比べ安価であることと大容量であることである．しかし，3D の NAND などの登場による SSD の大容量化，生産コストの減少により，SSD は安価化傾向にある．

HDD と SSD の違いは様々あるが，その一つが，SSD にはどのくらい使用できるかの書換え寿命回数があり，それが性能や機能により変化することである. その対策として，あらかじめ一定量の領域は予備として使わずに，未使用領域のまま残しておき，書換え寿命を延長する対策や処理速度の向上を図るという方法がある．この一定量の領域は Spare Capacity や Over Provisioned Capacity と呼ばれ，OS やユーザーからは一般的にアクセスすることができない．一般的にアクセスすることができないとは，その領域にファイルを保存する, フォレンジックツールでデータ抽出する，といったことができないことを示す意味する．また，SSD は HDD よりも，削除してしまったデータの復元がしにくいという報告もある．

本稿ではデジタル・フォレンジックの観点から，HDD と SSD の違いについて検証し，Spare Capacity や Over Provisioned Capacity からデータの復元について考察したい. 本稿では，まず，デジタル・フォレンジックにおけるデータ復元について HDD の場合と SSD の場合についてを比較する．ここでは大別して，Trim 機能によるデータ復元の差異についての検討と，予備の領域からのデータ復元について考察する. その後, SSD のアーキテクチャについて述べ，実際に Spare Capacity（Spare Capacity/Area）の調査を行う．

†1 情報セキュリティ大学院大学　博士前期課程
Graduate School of Information Security Institute of Information Security†2 情報セキュリティ大学院大学　教授
Graduate School of Information Security Institute of Information Security

a SSD 市場の 2017 年までの平均成長率は 39．2%　IDC 予測, http://www.itmedia．co．jp/enterprise/articles/1402/21/news092．html，2015 年 6 月アクセス

その後, 結果から判明したことと, Over Provisioned Capacity からの新たなデータ抽出手法について述べる．そして最後に，この調査全体に対するまとめを述べる．

2. デジタル・フォレンジックについて

本章では，デジタル・フォレンジックの定義とプロセスについてまとめる．

2.1 デジタル・フォレンジックとは

今日では，社会生活のあらゆる場面でパソコンや携帯電話・スマートフォンなどの IT 機器の利用が進んでおり，情報の大半は電子化され，IT 機器やサーバなどのネットワーク機器に蓄積されているのが実情である．営業秘密等も例外ではなく，デジタル・フォレンジックは，犯罪捜査，内部不正の調査，システムの不正利用調査，情報漏洩調査，公益通報への対応等の実態解明の場において，デジタルデータや通信記録の解析を行ううえで重要な役割を果たしている[1].

デジタル・フォレンジックというとは，インシデントレスポンスや法的紛争・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，電磁的記録の改ざん・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・技術のことを指す言葉である[2].

2.2 プロセス

デジタル・フォレンジックのプロセスは，

ⅰ)対象パソコンの特定
ⅱ)証拠保全
ⅲ)解析（削除ファイル・隠蔽ファイルの復元，該当ファイルの抽出，パーソナルコンピュータ利用の時系列調査等）
ⅳ)報告書作成

の流れで行うが，ⅲ）解析（削除ファイルの復元）については，様々な種類があるため，HDD と SSD の違いについて以下に分類した．

3. HDD と SSD のデータ復元の差異について

本章では，データの復元について，特にデジタル・フォレンジックの観点から調査した結果をまとめる．HDD と SSD では，データの復元を行った場合にどのように差異があるのか，先行研究を参照し述べる．

3.1 SSD 上の消去ファイルの復元可能性の実験と評価

山前は，SSD のディレクトリエントリからのファイル復元について研究し, データの復元及び SSD 本体を廃棄する時の安全性について評価している[3]. その結果, SSD には，不要になったデータを指示し消去するための機能である「Trim」有効時は，削除後 1 時間以内にほぼすべてのデータが残らないことを示している．OS が管理する最小単位であるクラスタが未使用の場合，消去対象 Block になった場合に自動的に発行されるもの．Trim コマンドの発行により，SSD を効率的に使用するためのガベージコレクションや，実際のデータ消去“0x00 上書き”を行うリフレッシュ処理が作動する．

また，Trim 無効時は，データの多くは削除してから一日しか残っていない（24 時間ですべて復元できなくなった）ことがわかった．これらは，ファイルサイズや拡張子，OS による大きな差異は見られないとしている．なお，ここでの復元とは，完全にデータがファイルとして復元されたもののみを示している．

3.2 ディレクトリエントリ

NTFS，FAT などのファイルシステムでは，ファイルはデータ本体とメタデータに分けて管理されている．ディレクトリエントリとは，このメタデータなどを管理している領域である．このメタデータ内には配置情報があり，これはデータ本体がメディア上のどの位置にあるかを保持している．言い換えれば各セクタがどのファイルによって占有されているか，あるいは空き領域となっているかどうかは，ディレクトリエントリによって管理されている．

ファイルの削除は通常，OS 内ではメタデータ内の削除，特に重要な配置情報の削除によって行われる．そのため，データ本体の各クラスタ内のデータは消去されることはないので，新規ファイルの作成や既存ファイルの更新などによってそのクラスタが再利用されるまでの間は，古いデータがそのまま残っている．よって，メタデータ内の配置情報を適切に再構築することができれば，ファイルは削除状態から復活が可能である．前述の，山前による SSD 上の消去ファイルの復元可能性は，ディレクトリエントリからのファイル復元（文中では，完全復元，と出ている）について実験と評価を行っている．

3.3 未使用領域などからのシグネチャ検索

ディレクトリエントリからの復元が不可能な場合でも，ファイルの復元が可能なケースが存在する．それは，メタデータ等の管理領域の情報がなくても未使用領域などからデータを復元する方法である．また，データベースの中にも同様に，削除したデータを復元できるものもある．例として，一般的なカメラやスマートフォンで撮影された画像は「JPEG 画像」と呼ばれ，拡張子が「. jpg」となっている．このデータは，バイナリで見た場合先頭が必ず「FFD8・・・」と始まり，最後が「・・・FFD9」となっており，中のデータ配列についても規格が決まっている．この部分を抽出すると，ファイル名や更新日時などの管理データはないが，画像自体のデータは復元できることがある．

この領域からのデータ復元については，上記「3. 2」の Trim の動作･タイミングによって異なるため, HDD と SSD の違いは，機種と設定に依存する．

3.4 ファイルスラック領域

上記のシグネチャ検索よりも小さな領域ではあるが，復元の可能性がある．2014 年の遠隔操作事件の公判において

もその言葉が出たといわれており，スラック領域からのデータ抽出である．ファイルスラック領域とは，データの終端とクラスタやボリュームの終端の間のことである．NTFS でいう 1 セクタは，512byte（一部，4Kbyte のものもある）であり，その中にある実データ以外のデータがスラック領域に存在する．

SDD においては，扱うことのできる最小単位は，4Kbyte，8Kbyte など，製品によって様々であり（4．1 で詳細を示す），HDD とは大きく異なる． この領域からのデータ復元についても，上記「3．2」の Trim の動作・タイミングによって異なるため，HDD と SSD の違いについては不明である．Trim の発行により，リフレッシュがかかることで，3．3 の未使用領域などからのシグネチャ検索と同じであるとも予測できるが，同時にガベージコレクションなどの機能があるため，詳細は機種と設定による．

3.5 外部領域

OS やユーザーが通常アクセスできないが，データが存在する領域がある．HDD 及び SSD に対して設定が可能な保護領域と，SSD にしか存在しない「Spare Capacity と Over Provisioned Capacity」がある．

3.5.1 保護領域

HPA（Host Protected Area：ホスト保護領域），DCO（Drive Configuration Overlay：装置構成オーバーレイ）といった機能で領域を区切り，データ取得を不可能にすることもできる．HPA については，ATA 規格のディスクにおいての HDD そのものが備えるセキュア消去という機能を用いることで完全なデータ削除が可能である．また，DCO については，エンハンストセキュア消去で代替セクタも含めたデータの削除が可能である．この領域は，ストレージの使用方法などに依存する．また，HDD は物理アドレスと論理アドレスが同じものを示すが，SSD は物理アドレスと論理アドレスが常に同じではないため，セキュア消去の動作が異なる．

3.5.2 Spare Capacity と Over Provisioned Capacity

SSD を効率的に使用するため，SSD には予備の領域が存在し，Spare Capacity や Over Provisioned Capacity と表記されることが多い．一般的には，SSD 全体の容量の 10～20%と言われており，OS やユーザーからはアクセスできない領域である．この領域の呼ばれ方は様々で，Spare Capacity，Over Provisioned Capacity，冗長エリア，余剰メモリ，余剰記憶領域，余剰容量，性能設定領域，などとも呼ばれる．今回の調査では，この領域について調査・検証する．

4. NAND フラッシュメモリの SSD

本章では，SSD の NAND フラッシュメモリの概要について，HDD などとの差異，アーキテクチャについて調査した結果をまとめる．

一般的に販売されている SSD は NAND フラッシュのものがほとんであり，購入の際の選択肢及び購入基準として考えられるのは，価格，容量，速度性能，耐久性能，データ信頼性などがあるが，今回の調査を行う上で HDD と比較とした場合は以下の点が特徴的である．

・容量が大きいほど読込み速度などが速い
・長時間使うと遅くなり（対策あり．後述）
・寿命がある（対策あり．後述）

この 3 点において，その理由を以下に述べる．

4.1 アーキテクチャ

NAND フラッシュの SSD の詳細構造は製品により異なる．また，NAND 以外では，ファームウェア，BIOS や組込みシステムなどに使われることが多い NOR フラッシュがあるがここでは触れない．NAND フラッシュの SSD の構成の一例を図 1 に示す．

図 1　MacBookAir（2015）の SSD（※出典：ifixit）

左から，NAND 型フラッシュメモリ 16GB×8 個，512MB の DRAM，フラッシュコントローラーである．最近は，DRAM の代わりに SDRAM を使用するものも増えてきている．また，製品によっては，DRAM を一切使わず，コントローラー内部のキャッシュと Spare Capacity 用に確保された NAND チップ（NAND 型フラッシュメモリ）でまかなう SSD も存在する．さらに，アーキテクチャとしては，以下のようになっている．

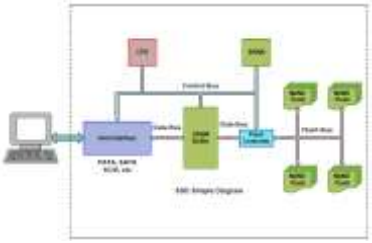

図 2　SSD のアーキテクチャ（※出典：imation）

NAND のアーキテクチャの例について述べる．まず，Flash Controller がフラッシュメモリのアドレッシング，プログラミング，消去，読込みなどの制御を行う．DRAM は，データが転送され処理する．CPU は，SSD のフラッシュメモリへの読書きを調整介入する．SRAM は，テーブルや論理アドレスと物理アドレスマッピングなどフラッシュ交換レイヤである FTL を用いて行う．そして，NAND チップがあり，その中は Plane と呼ばれる複数の Block からなっている．NAND は，記憶素子 1 個単位での処理はできない仕組みとなっている．データ書込みの Write 処理とデータ読

込みの Read 処理は，SSD が処理できる最小短いである 1Page（2，4，8，16Kbyte のいずれかであるが，製品によって異なる）単位，Erase 処理は 1Block（512Kbyte が多いが，製品によってはそれ以上のものもある）単位となっている．SSD は，素子の処理の仕方のため直接 Erase 処理を行うことができないことと，読書きとの処理単位の違いから，様々な機能を有している．アーキテクチャのこの点が，HDD とは大きく異なる点である．

4.2 機能，動作

SSD は，フラッシュコントローラーに様々な機能が実装されている．Erase 処理による，処理速度の遅延，寿命対策として，いくつかの機能を述べる．

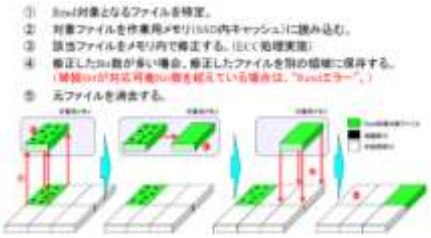

図３　Erase 処理（出典：日系エレクトロニクス）

前述したように，NAND チップは記憶素子 1 個単位での処理ができないため，直接上書きすることができない．したがって，Re-Write 処理（修正，上書き）の場合，Read-Modify-Write-Erase 処理の一連の流れで，一つの Re-Write 処理となる．

ここで NAND チップには書き換え可能回数が存在し，Write/Erase のたびに，電子が絶縁体を通過する程度の電圧をかけているため絶縁性が劣化していく．一定回数を超えると，傷ついた絶縁体では，フローティングゲートに注入された電子を保持できなくなる．対策としてすべての SSD に実装されている機能が Wear Leveling である．Wear Leveling とは，NAND への書き込み回数の平準化のことであり，領域の使い方の効率を上げ，寿命を延ばしている．実装方法はベンダーにより異なる．また，一般的には，Write と Erase という 2 回の書き換えを行うよりも，Erase 部分の Block を消去対象 Block として実際には書き換えを行わないことで，寿命を延ばしている製品もある．

こういった Block の消去は時間がかかる操作（書き込みの何十倍もかかる）であり，パフォーマンスを劣化させる原因になる．そのため，適切な空き Block を常に用意しておくことが重要である．空き Block が少ないと，セルへの書き込み回数が増えることになり，SSD が短命化してしまう．このような事態を避けるために，あらかじめ一定量の領域（Spare Capacity や Over Provisioned Capacity）は使わずに，未使用領域のまま残しておくことを Over Provisioned という．そして，そのための領域を Over Provisioned Capacity という．製品にもよるが，あらかじめ 5～20%程度（サーバ向け製品では 20%を超えるものもある）はこの領域のために予約されており，OS やユーザーが利用することはできない．この領域にある消去対象 Block をターゲットに，データ復元の可能性がある．

4.3 Spare Capacity と Over Provisioned Capacity

Spare Capacity 及び Over Provisioned Capacity という言葉に関しては，ベンダー毎によって表現の仕方が異なるが，ここで Spare Capacity と Over Provisioned Capacity という言葉を分けて使用する．その Spare Capacity と Over Provisioned Capacity として分け方を述べる．

4.3.1 Spare Capacity

一般的な SSD は，2 進法表示（Binary Gigabytes）と販売のための表記容量である IDEMA 標準容量の差を，Spare Capacity（交代領域）用として使用していることが多い[5]．今まで，ディスクの容量について詳細を確認していなかったため，OS の管理情報及びフォレンジックツールを用いて正確な容量について確認を行った．なお，調査を行った SSD は，「256GB」と表記されていたものである．ここで確認したいことは 2 点である．1 点目は，OS で見ることのできる容量とフォレンジックツールで見ることのできる容量の差を確認することである．2 点目は，SSD の表記と実容量に差があるかを確認することである．

図４　SSD の容量（デバイスマネージャー）

パーソナルコンピュータ上で容量を参照にする場合，回復用パーティションや予約領域などがあるため，デバイスマネージャーの Disk Device のプロパティで容量を確認した．この SSD では，容量は「244，198MB」と表示されている．

図５　SSD の容量（Forensic Tool）

次に，Access Data 社の Forensic Tool である FTK Imager（Ver3．2．0．0）を使用して，通常アクセスできる全領域を見てみた．全領域の最終論理アドレスが，16 進数で「3b9e6557af」となっているため，これを 10 進数にすると「256，060，512，160」（単位：byte）となり容量が判明する．MiB で計算（/1024^2）すると「244，198MiB」となり，上記の OS の管理情報と同じ容量であった．この結果から，
・フォレンジックツールなどを使用する方法では Spare Capacity や Over Provisioned Capacity へはアクセスできないことを確認した．

・2 進法表示である IDEMA 標準容量の差である部分が Spare Capacity であるとしていたが，この SSD に Spare Capacity があるかはこの手法のみでは不明であることがわかった．

後者の不明であることの理由に関して，HDD においても同様の確認を行ったところ，デバイスマネージャーでは「476，940MB」，フォレンジックツールでは「500，107，857，680byte = 476，940MiB」となっており，同じ容量であった．他の SSD 及び HDD と SSD を組み合わせた SSHD（Solid State Hybrid Drive）でも確認してみたが，同様の結果であった．

以上のように，あるパーソナルコンピュータ内蔵の SSD について，表記の容量と，実際に OS 及びユーザーからアクセスできる容量の差について確認した．その結果から判明したことを 2 点述べる．
・256GB という容量表記は，実際は 238GB のことである．「256, 000, 000, 000byte(Manufacturing Company) / 1, 073, 741，824 byte(OS： 1GB) = 238GB」のため
・およそ 18GB 分の容量の差は，Spare Capacity であり，ユーザーエリアを除いた追加ブロックである．

とのことから，Spare Capacity について確認することができた．また，Spare Capacity についてはセキュアイレースでなければデータの削除はできないことも判明した．（注意点として，容量表記とセキュアイレースについて，本研究では，まだこの 1 社しか確認していない．）

4.3.2 余剰領域/Over Provisioned Capacity

Over Provisioned Capacity については以下の効果などを狙ったものであり，物理的には Spare Capacity と同じ NAND チップを示す．

・ガベージコレクション効率向上
・速度向上（速度劣化防止）
・製品寿命延伸

Spare Capacity と Over Provisioned Capacity は，物理的な領域としては同じだが，2 つを別のものとする．

フラッシュメモリの Spare Capacity 及び Over Provisioned Capacity からのデータ抽出については，対策も施されている．その対策とは，データ全体への暗号化や，ローレベルフォーマットなどである．しかし，Michael Wei らによると，SSD のおよそ 4～75%のデータが復元可能であり，USB メモリについても消去の失敗により 0．57～84．9%のデータがアクセス可能だったとされている[4]．その理由は，ATA/Serial ATA ストレージ向けの，情報漏えいを防止する目的に用意されたコマンドであり，ディスク全域をランダムの値で上書きをする，Security Erase Unit コマンドの実装に不備があるためだとされている．現在は，SSD の性能低下対策に用いられることも多い．

また，IPA の「デジタル複合機のセキュリティに関する調査報告」では，SSD 搭載による情報漏えいの問題として，デジタル複合機の内蔵 SSD の廃棄時・返却時以降の保護資産の漏えいリスクについて，上記の実装不備と Over Provisioned Capacity からのデータ復元のリスク及び，攻撃者からの視点について述べている[7]．

4.3.3 予備の領域の OS での設定例

予備の領域をユーザーで設定できる SSD もある．Samsung 製 SSD と Intel 製 SSD には，それぞれ同社製造のフリーソフトウェアで予備の領域が設定できるものだ．Samsung 製の場合の，「Magician」というフリーソフトウェアを使用する例を以下に示す．

図６　Magician 上での設定変更（※出典：Samsung）

上記においては，上級者向けの機能として，予備の領域をおよそ 10%程度増加させることにより，寿命などを延ばす方法である．この領域は，Windows 上からは未割当領域として見えるようになる「Over Provisioned 設定」との記載があった．そのため，こういった予備の領域の増加設定部分について確認する必要がある．

この設定した領域にアクセス可能であれば，ベンダーの機能により，予備の領域からのデータ復元の可能性が高まる．また，「4．3　機能」で述べたものと同様に，OS やユーザーからのアクセスが不可能であった場合，OS から制御コントローラーへコマンドを送りこんでファームウェアの設定をしている可能性が高いため，そのファームウェアへ送っているコマンドがわかれば，何かしらのアクセス手法を検討できる蓋然性が高い．

5. データ抽出手法の提案

前述した Over Provisioned Capacity からのデータ抽出手法は, チップオフのダンプ作業により実現できる. しかし, チップオフには，デバイスの破壊を伴うことが多い，SSD 全体の暗号化が施してあるとデータの可視化が不可能になるというデメリットもある．そこで，これらのデメリットを回避できる新たな 4 つのデータ抽出手法を提案する．

5.1 ファームウェアを改変してのデータ抽出

ファームウェアとは，永続性メモリに保存された低レイヤで動作するソフトウェアのことであり，基本システムを動作させ，さらに上位のレベルのソフトウェアにサービスとインターフェースを提供している. SSD においても, Trim コマンドの発行やガベージコレクション，論理・物理アドレスのマッピングなど，様々な機能を有している（機種によっては, ファームウェアとは別に CPU を持つものも存在し, そこでマッピングなどを制御するものも存在する）. このファームウェアは容易に変更できない．しかし，ファームウェアの動作の中や，他のソフトウェアと情報をやりとりする方法の仲に脆弱性が存在することが多くある．ファームウェアのリバースエンジニアリングにより，コードを研究し，実行ロジックの中に弱点や脆弱性を見つけ出すことが可能になる場合がある．そうすることで，ファームウェアの制限を破ることが可能になる．

SSD のデータ抽出方法として，4 章でも前述したファームウェアの利用を考えた．SSD ファームウェアのアップデートデータのバイナリを解析し，ファームウェアアップデートデータの改変を行うことで，Over Provisioned Capacity から読取りを試みるという手法が有効と考えられる．なぜなら，Over Provisioned Capacity についてはファームウェアが管理，制御しているためである．

5.2 Boot loader を利用してのデータ抽出

Boot loader とは，コンピュータの起動直後に動作し，OS をディスクから読み込んで起動するプログラムのことである．この Boot loader を利用すれば，デバイス起動時のデータを読み込むことが可能であり，それを利用してデータ抽出を行うことが可能となる．類似例として，システムが電力消費を抑えるスリープモードやスタンバイ状態にあるような場合に暗号化鍵の情報をシステムのメモリから抽出するような攻撃方法である Cold Boot Attacks というものがある．一般に，Boot loader と Cold Boot Attacks の違いは，事前に対象デバイスのロック解除があるかないかである．Boot loader においては，事前のロック解除が必要とされているが，そうではないケースも存在する．

一例として，スマートフォンからのデータ抽出を行う場合において，パスコードが不明であっても，Boot loader を利用することにより，Boot 時の情報を読取り，エージェントを入れることなく，フィジカルダンプデータの取得が可能である．つまり，Boot loader を利用することにより，証拠となる元のデータに変更を加えることなく，デバイスの全領域のデータ抽出が可能となる．

5.3 Console 端子からのデータ抽出

Console 端子とは, 本体以外の入出力装置のことである．PC ならば，モニターやキーボードなどが該当する．ゲーム機器などでは，Console 端子からのデータ抽出が行われるケースが多い（PS3，Xbox など）．b Console 端子からのデータ抽出は，中のストレージデバイスを取り出さずにデータの抽出が可能であり，デジタル・フォレンジックの手法の一つとして有効である．現在，組込みシステムにおいても，Console Forensic の研究が行われている．

5.4 JTAG 端子からのデータ抽出

JTAG とは，Joint Test Action Group：IEEE1149．1 標準テストアクセスポートとして標準化されている規格のことである．対象がスマートフォン Samsung Galaxy S3 (SGH-I747M)の例では，対象スマートフォンの NAND フラッシュの Physical Image の取得は，JTAG 端子からのデータ抽出という手法以外にないと言われている. c 多くのデバイスには，この JTAG が存在し，JTAG Forensic という言葉があるように，データ抽出の際の 1 つの選択肢となっている．それを，SSD にも利用できた場合，有効性が高い．

6. まとめ

SSD の Over Provisioned Capacity を除く領域では，SSD は HDD よりもファイルの完全復元ができない．それは，Trim 機能により，通常の手法ではデータ抽出が不可能な Over Provisioned Capacity にデータが蓄積されるためである．

しかし，SSD のすべての領域では，HDD よりも多くのデータ抽出が可能である．Spare Capacity および Over Provisioned Capacity という予備の領域に多くのデータが残っているためである．およそ，製品表示容量の 10～20%がその領域にあたる．この領域を解析することで，より多くのデータ抽出およびデータ復元が可能になる．

そこで本稿では，その予備の領域からデータを抽出することを可能とする新たな手法を 4 つ提案した．新たな 4 つの手法の有効性については今後の課題としたい．これらの手法が可能になった場合，より多くのデータ抽出およびデータの可視化が可能になるため有用的であると考える．

7. 参考文献

1）羽室 英太郎“デジタル・フォレンジック概論～フォレンジックの基礎と活用ガイド” 2015 年 4 月出版

b Scott Conrad, Greg Dorn, Philip Craiger “Forensic Analysis of a PlayStation 3 Console” Advances in Digital Forensics VI
Volume 337 of the series IFIP Advances in Information and Communication Technology pp 65-76

c JTAG Samsung Galaxy S3，http://forensicswik，2015 年 7 月アクセス

２）佐々木良一　“改訂版デジタル・フォレンジック辞典” 日科技連　2014 年 4 月出版
３）山前碧　“SSD 上の消去ファイルの復元可能性の実験と評価” 2015-CSEC-68 No. 39
４）Xiao-Yu Hu ら“Write Amplification Analysis in Flash-Based Solid State Drives” 2009-ACM
５）Michael Wei, Laura M. Grupp, Frederick E. Spada, Steven Swanson “Reliably Erasing Data From Flash-Based Solid State Drives” 9th USENIX Conference on File and Storage Technologies (FAST '11), Feb 2011