「攻めのデジタル・フォレンジック」

不正の解明可否が分かれた
デジタル・フォレンジック基点での境界線

第14回デジタル・フォレンジック・コミュニティ2017 in TOKYO
大阪データ復旧（株）　下垣内　太（しもがいと　だい）

破壊されたハードディスクのデータ復旧と解析

被疑者に破壊され、データ保全が不可能と判断された
パソコンを解析し、犯行時間帯の行動履歴を時系列で
解明した際の技術的工程および捜査機関との連携の過程

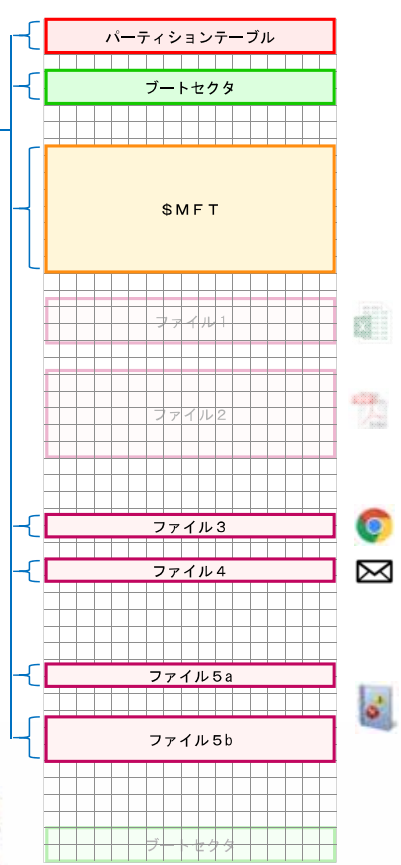
証拠隠滅を狙って破壊されたHDD

注）この写真のハードディスクドライブは、実際の事件証拠品の破壊状況を下垣内太が再現したものです。いずれの写真も本物の証拠品ではございません。

１GBだけ読める状況で手作業を選ぶメリット

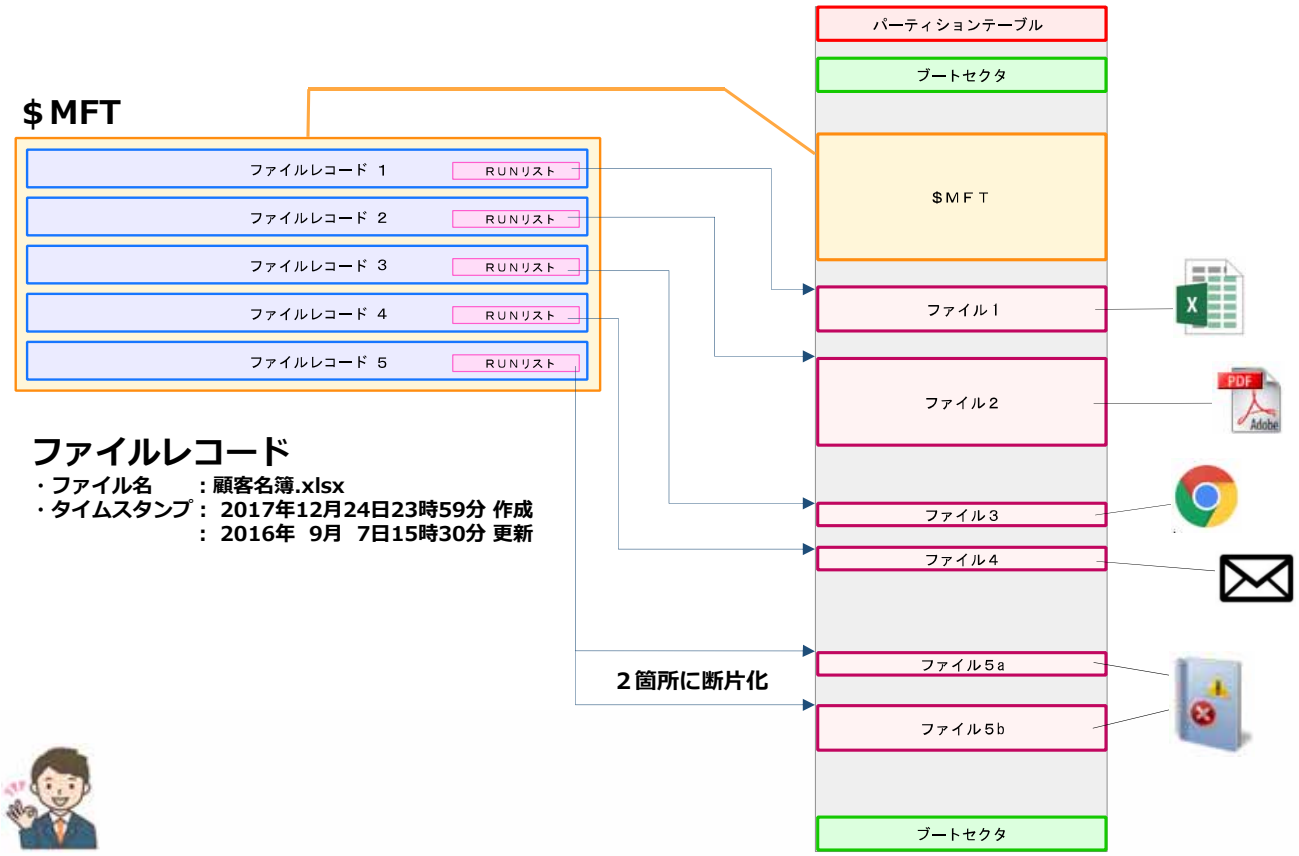
先頭から連続１GB

ピンポイントの合計１GB



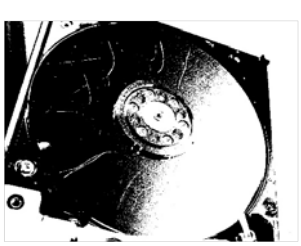
証拠確保
- ウェブ履歴
- メッセージ
- イベントログ

ＮＴＦＳのデータ配置



Dai Shimogaito
OSAKA DATA RECOVERY

最難関はプラッタ表層ダメージの克服



ファームウェアレベルでの調整と改造

&

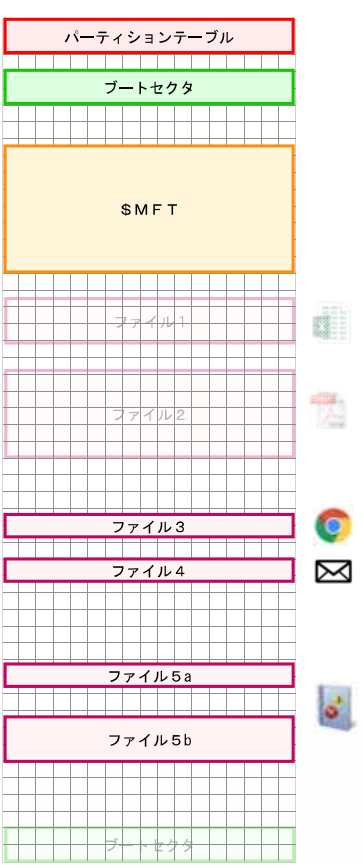
磁気ディスク表層ダメージの低減化

&

部品交換による一時修繕（通常のデータ復旧技術）

ヘッドアセンブリ交換

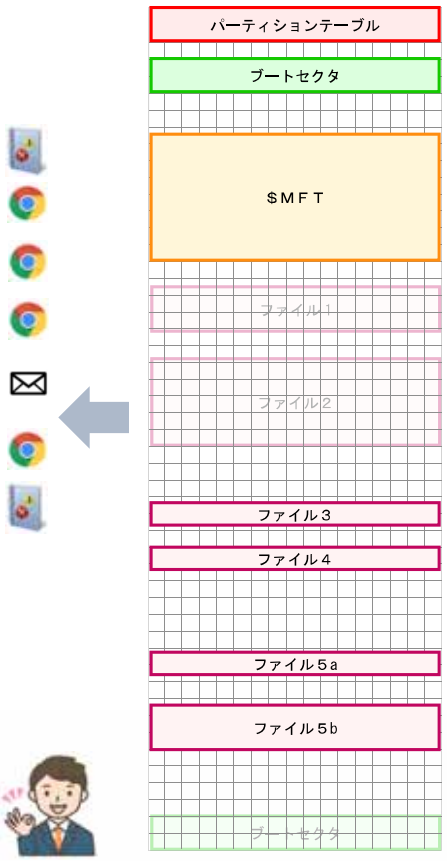
制御基板修復



Dai Shimogaito
OSAKA DATA RECOVERY

収集したデータを時系列化し、対象者の行動経緯を把握

時刻	出来事	ソース
10時58分01秒	被疑者が１２３号室を訪問。玄関内に入り扉が閉まった。	防犯カメラ
11時07分16秒	パソコン起動	イベントログ
12時05分47秒	ブラウザで"呼吸停止　頭部ケガ"と検索	Web 検索履歴
12時08分32秒	ブラウザで"応急処置"と検索	Web 検索履歴
12時09分23秒	Webページ「応急手当の仕方」を閲覧。	Web 閲覧履歴
12時11分55秒	被害者宛に被害者知人Aからメールが届く。 「今日一緒にランチする予定はキャンセル？１時までは店で待つわ」	メッセージ
12時15分03秒	ブラウザで"指紋の消し方"と検索	Web 検索履歴
12時25分41秒	パソコンシャットダウン	イベントログ
13時18分10秒	被疑者が１２３号室を出た。	防犯カメラ
20時48分	被害者知人A、１１９番救急車要請	捜査情報
20時56分	救急車到着	捜査情報



日時情報と人の行為がペアになるデータを
ピンポイントで収集

Dai Shimogaito
OSAKA DATA RECOVERY

解析対象を特化しすぎると重要証拠を見落とす

```
1659896478... 72 63 65 53 65 74 02 00  00 00 58 00 00 00 0C 00  rceSet    X
1659896479... 00 00 67 53 79 73 74 65  6D 2E 44 72 61 77 69 6E    gSystem.Drawin
1659896479... 67 2E 53 69 7A 65 46 2C  20 53 79 73 74 65 6D 2E  g.SizeF, System.
1659896479... 44 72 61 77 69 6E 67 2C  20 56 65 72 73 69 6F 6E  Drawing, Version
1659896479... 3D 32 2E 30 2E 30 2E 30  2C 20 43 75 6C 74 75 72  =2.0.0.0, Cultur
1659896479... 65 3D 6E 65 75 74 72 61  6C 2C 20 50 75 62 6C 69  e=neutral, Publi
1659896479... 63 4B 65 79 54 6F 6B 65  6E 3D 62 30 33 66 35 66  cKeyToken=b03f5f
1659896480... 37 66 31 31 64 35 30 61  33 61 66 53 79 73 74 65  7f11d50a3afSyste
1659896480... 6D 2E 44 72 61 77 69 6E  67 2E 53 69 7A 65 2C 20  m.Drawing.Size,
1659896481... 61 77 69 6E 67 2C 20 56  65 72 73 69 6F 6E 3D 32  ewing, Version=2
1659896481... 2E 30 2E 30 2E 30 2C 20  43 75 6C 74 75 72 65 3D  .0.0.0, Culture=
1659896481... 6E 65 75 74 72 61 6C 2C  20 50 75 62 6C 69 63 4B  neutral, PublicK
1659896481... 65 79 54 6F 6B 65 6E 3D  62 30 33 66 35 66 37 66  eyToken=b03f5f7f
1659896482... 31 31 64 35 30 61 33 61  75 53 79 73 74 65 6D 2E  11d50a3auSystem.
1659896482... 57 69 6E 64 6F 77 73 2E  46 6F 72 6D 73 2E 50 61  Windows.Forms.Pa
1659896482... 64 64 69 6E 67 2C 20 53  79 73 74 65 6D 2E 57 69  dding, System.Wi
1659896482... 6E 64 6F 77 73 2E 46 6F  72 6D 73 2C 20 56 65 72  ndows.Forms, Ver
1659896482... 73 69 6F 6E 3D 32 2E 30  2E 30 2E 30 2C 20 43 75  sion=2.0.0.0, Cu
1659896482... 6C 74 75 72 65 3D 6E 65  75 74 72 61 6C 2C 20 50  lture=neutral, P
```

内部不正（詐欺）調査にて、経営者が指定した項目
以外のデータについても調査したところ、
関連する詐欺事件全体の主犯格が判明した実例

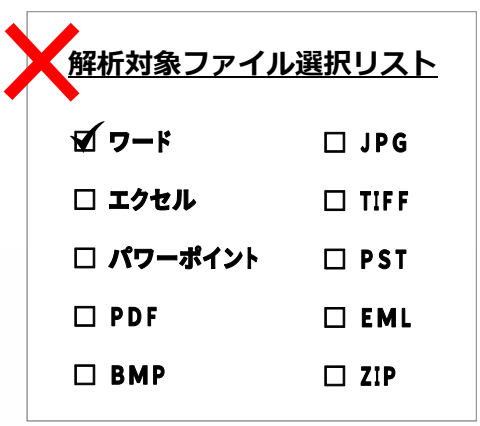
Dai Shimogaito
OSAKA DATA RECOVERY

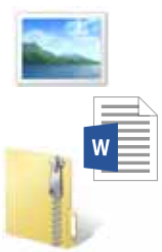
解析対象を特化しすぎると重要証拠を見落とす

依頼人のリクエスト 削除されたワード文書を探してくれないか？

（1） 社長が知らない契約書を元従業員が作成し、売買成立していたことが発覚
（2） 社内の契約書は全てMS-Word文書であった
（3） まだ発覚していない不正契約が他にもあったのではないか？

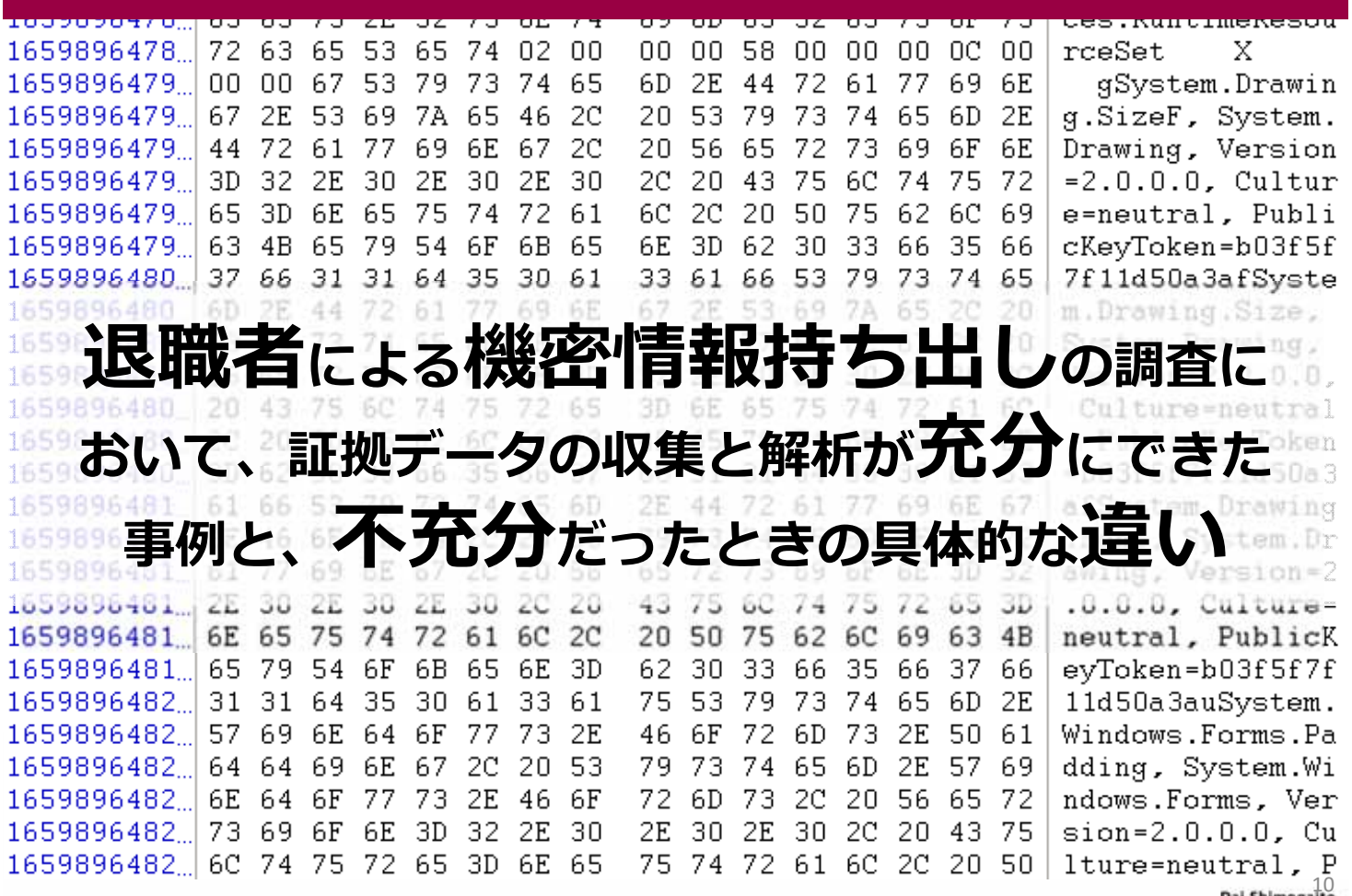
解析後、MS-Wordデータは検出されず。だが、真犯人と未発覚の不正契約が判明。





Dai Shimogaito
OSAKA DATA RECOVERY

不正の解明可否が分かれたボーダーライン



退職者による機密情報持ち出しの調査において、証拠データの収集と解析が充分にできた事例と、不充分だったときの具体的な違い

Dai Shimogaito
OSAKA DATA RECOVERY

不正の解明可否が分かれたボーダーライン（環境）

依頼人のリクエスト **退職者が機密情報を持ち出した証拠がほしい。**

◎

（１）　退職後、ＰＣは使用されずに保管されていた

（２）　社内のデータコピー監視ログと個人ＰＣの痕跡を照合できた

（３）　予め監視チームと、事案発生時の調査手順を想定していた

まずはＰＣデータの保全をしよう！  **早期ほど有用**

※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」 https://digitalforensic.jp/wp-content/uploads/2017/05/idf-guideline-6-20170509.pdf

×

（１）　ファイル削除から時間が経ち、ＰＣ使用が継続されていた

（２）　ＨＤＤでなくＳＳＤだった ※設定による

（３）　機密情報の持ち出しにパソコンが使用されていなかった

とりあえずＰＣ起動して調べてみよう！ **証拠が減る** 

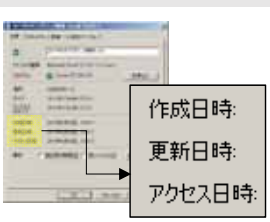
Dai Shimogaito
OSAKA DATA RECOVERY

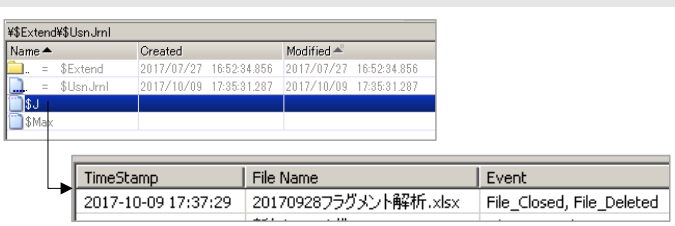
不正の解明可否が分かれたボーダーライン（解析）

依頼人のリクエスト **退職者が機密情報を持ち出した証拠がほしい。**

◎

（１）　ファイル削除日時が、ＵＳＮジャーナルに残されていた





◎

（２）　社内はWindowsだけなのに、Mac使用の痕跡が見つかった

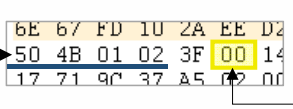
Mac特有の
リソースフォーク

Name	Created	Modified
.. = 調査回収ファイル	2017/10/09 16:57:53.750	2017/10/09 16:58:07.781
.. = 持ち出しファイル	2017/10/09 16:58:07.781	2017/10/09 16:58:07.801
_20170928フラグメント解析.xlsx	2017/10/09 16:58:07.801	2017/10/09 16:56:28.000
20170928フラグメント解析.xlsx	2017/10/09 16:58:07.801	2017/09/28 03:10:18.000

◎

（３）　社内はMacだけなのに、Windows使用の痕跡が見つかった

圧縮した際のOSの種類が、ZIPファイル内
セントラルディレクトリに記録されている



セントラルディレクトリヘッダ

セントラルディレクトリ
ヘッダから２バイト目

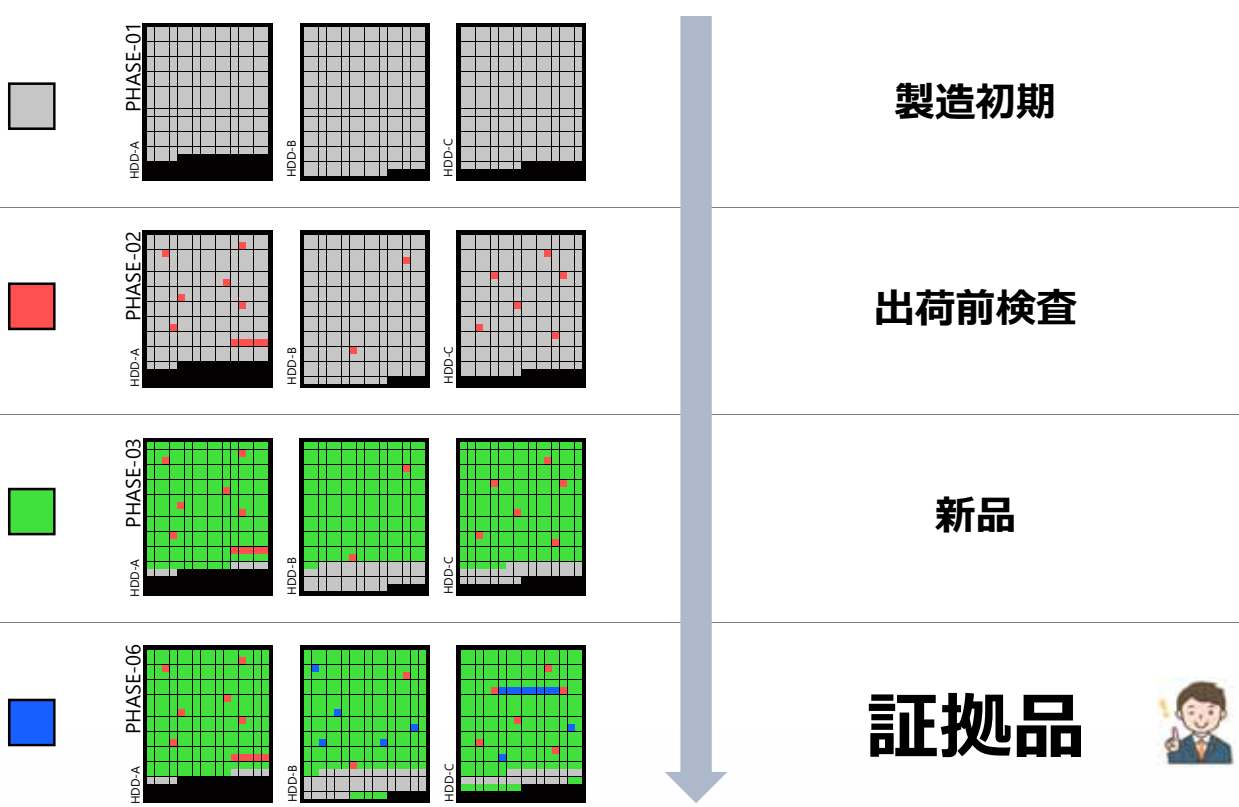
Dai Shimogaito
OSAKA DATA RECOVERY

ＨＤＤデータの保全と消去の対象範囲

”HDD や SSD に対する一定以上のレベルでの
データ抹消は現時点では不可能に近い”

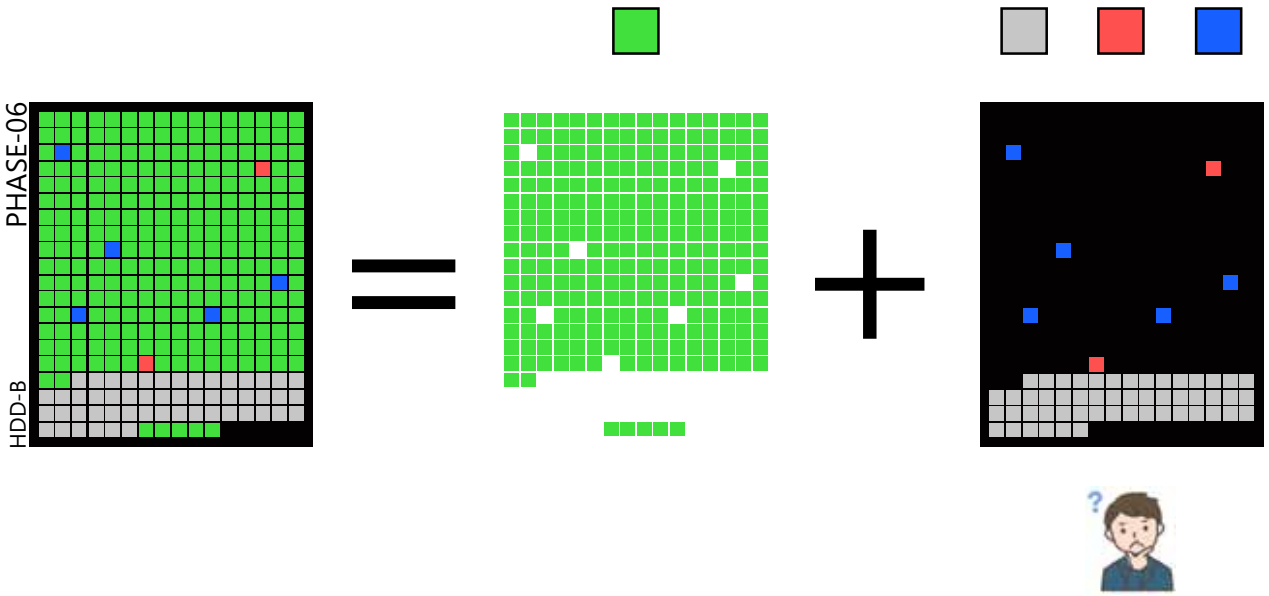
特定非営利活動法人デジタル・フォレンジック研究会 「データ消去」分科会
証拠保全先媒体のデータ抹消に関する報告書（2016年4月11日）より

物理セクタと論理セクタの構造



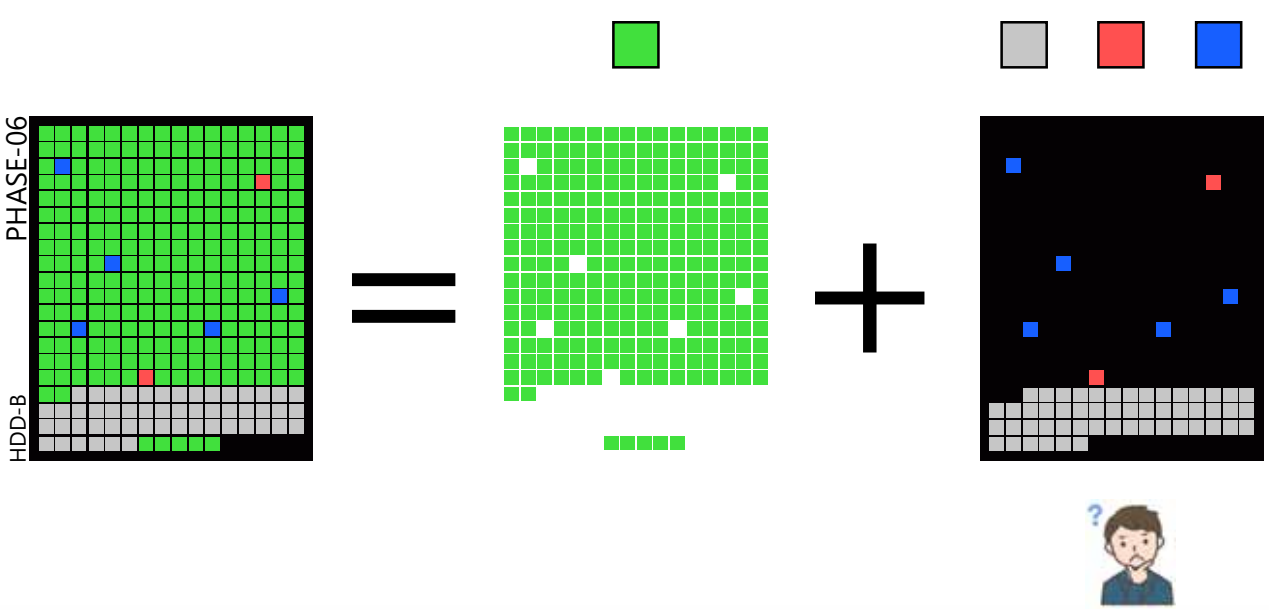
LBAが割り当てられていないセクタ
製造段階でLBAの割り当てが除外されたセクタ
LBAが割り当てられているセクタ
代替処理後の不良セクタ

保全解析の対象と非対象領域



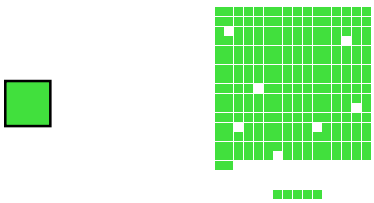
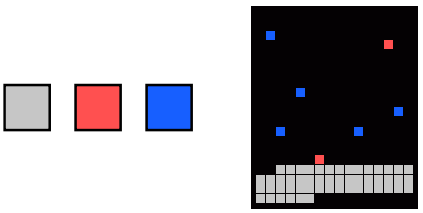
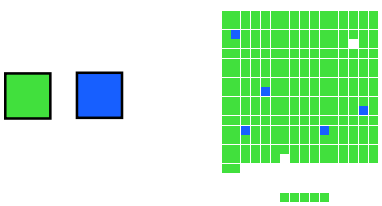
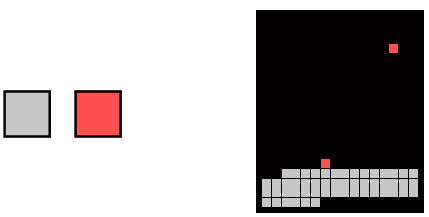
LBAが割り当てられていないセクタ
LBAが割り当てられているセクタ
製造段階でLBAの割り当てが除外されたセクタ
代替処理後の不良セクタ

データ消去の対象と非対象領域



LBAが割り当てられていないセクタ
LBAが割り当てられているセクタ
製造段階でLBAの割り当てが除外されたセクタ
代替処理後の不良セクタ

データ消去の対象と非対象領域

	消去可	消去不可
データ消去ソフト・ツール Secure Erase DoD方式（米国国防総省） グートマン方式（35回） ※物理破壊は除く		
Enhanced Secure Erase （NIST）		

参考文献

特定非営利活動法人デジタル・フォレンジック研究会「データ消去」分科会、証拠保全先媒体のデータ抹消に関する報告書(2016)
https://digitalforensic.jp/wp-content/uploads/2016/02/report.pdf

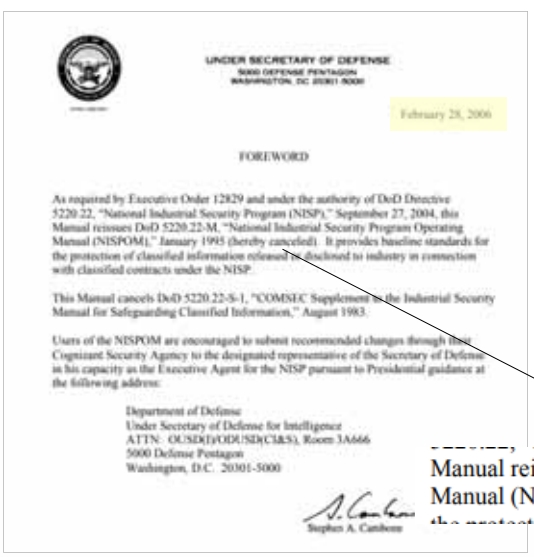
- LBAが割り当てられていないセクタ
- LBAが割り当てられているセクタ
- 製造段階でLBAの割り当てが除外されたセクタ
- 代替処理後の不良セクタ

ワイプ済みＨＤＤでも調査の余地はある

（１）　全セクタを完全消去するツールは無い　※物理破壊は別

（２）　不良セクタにはデータが残存

（３）　テロ対策レベルの解析余地はある



UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

February 28, 2006

FOREWORD

As required by Executive Order 12829 and under the authority of DoD Directive 5220.22, "National Industrial Security Program (NISP)," September 27, 2004, this Manual reissues DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," January 1995 (hereby canceled). It provides baseline standards for the protection of classified information released or disclosed to industry in connection with classified contracts under the NISP.

This Manual cancels DoD 5220.22-S-1, "COMSEC Supplement to the Industrial Security Manual for Safeguarding Classified Information," August 1983.

Users of the NISPOM are encouraged to submit recommended changes through their Cognizant Security Agency to the designated representative of the Secretary of Defense in his capacity as the Executive Agent for the NISP pursuant to Presidential guidance at the following address:

Department of Defense
Under Secretary of Defense for Intelligence
ATTN: OUSD(I)/ODUSD(C1&S), Room 3A666
5000 Defense Pentagon
Washington, D.C. 20301-5000

Stephen A. Cambone

Manual reissues DoD 5220.22-M, "National Industrial S
Manual (NISPOM)," January 1995 (hereby canceled). I

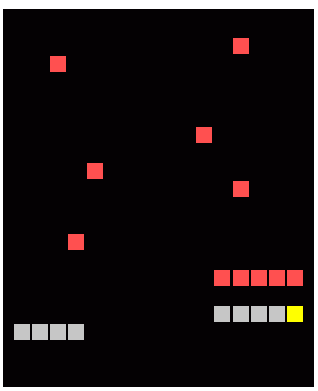
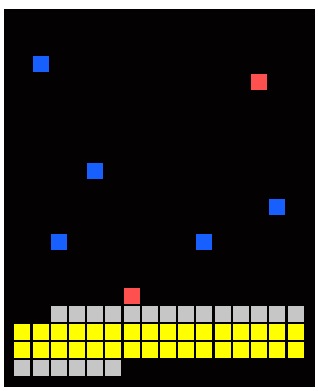
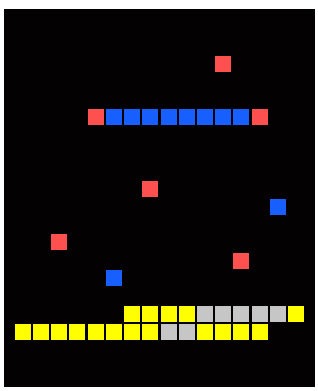
DoD（米国国防総省）準拠方式

DoD5220.22-M

2006年に破棄済み

悩ましい問題

データ消去

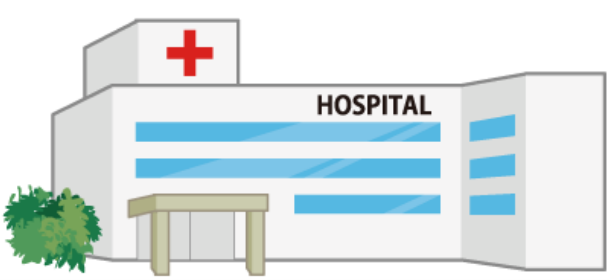




全セクタを**完全消去**できるソフトウェアは**無い**

Dai Shimogaito
OSAKA DATA RECOVERY

見えないセクタ、見えないデータとの闘い

サイバーテロ

Dai Shimogaito
OSAKA DATA RECOVERY

検討すべき課題

デジタル・フォレンジック

我々はHDDの全てのデータ領域を調べつくしました。

物理イメージはHDDの完全なる複製物です。

そうなんですね？

捜査機関　　裁判所

検討すべき課題

デジタル・フォレンジック

解決策（案）

全論理セクタの情報を調べました。

そうなんですね？

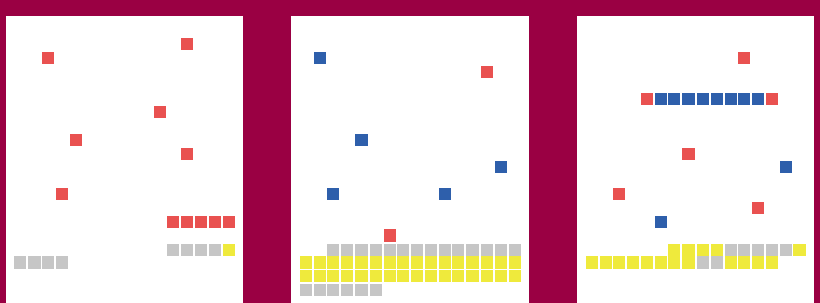
捜査機関　　裁判所

Dai Shimogaito
OSAKA DATA RECOVERY

製造物責任

消費者 & ユーザ（顧客）

ベンダ & メーカ



PARADAIS