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

デジタル・フォレンジック・コミュニティ2019 in 関西（２／１９）

アイフォレンセ日本データ復旧研究所（株）　大阪データ復旧
下垣内 太（しもがいと だい）

自己紹介

下垣内 太 （しもがいと だい）

大阪データ復旧 - 梅田・大阪駅前第4ビル
アイフォレンセ日本データ復旧研究所（株） 代表取締役

一般社団法人 日本データ復旧協会 常任理事
デジタル・フォレンジック研究会 会員

愛知県豊川市出身
愛知県立時習館高等学校卒
関西大学総合情報学部卒
1998年創業

データ復旧 – 故障したコンピュータからデータを救出

デジタル・フォレンジック調査 – 犯罪や不正事件の証拠品解析

サイバーセキュリティ研究 – HDDの隠しデータ領域

https://www.facebook.com/dai.shimogaito

壊された証拠品からのデータ復旧事例

壊された証拠品からのデータ復旧事例

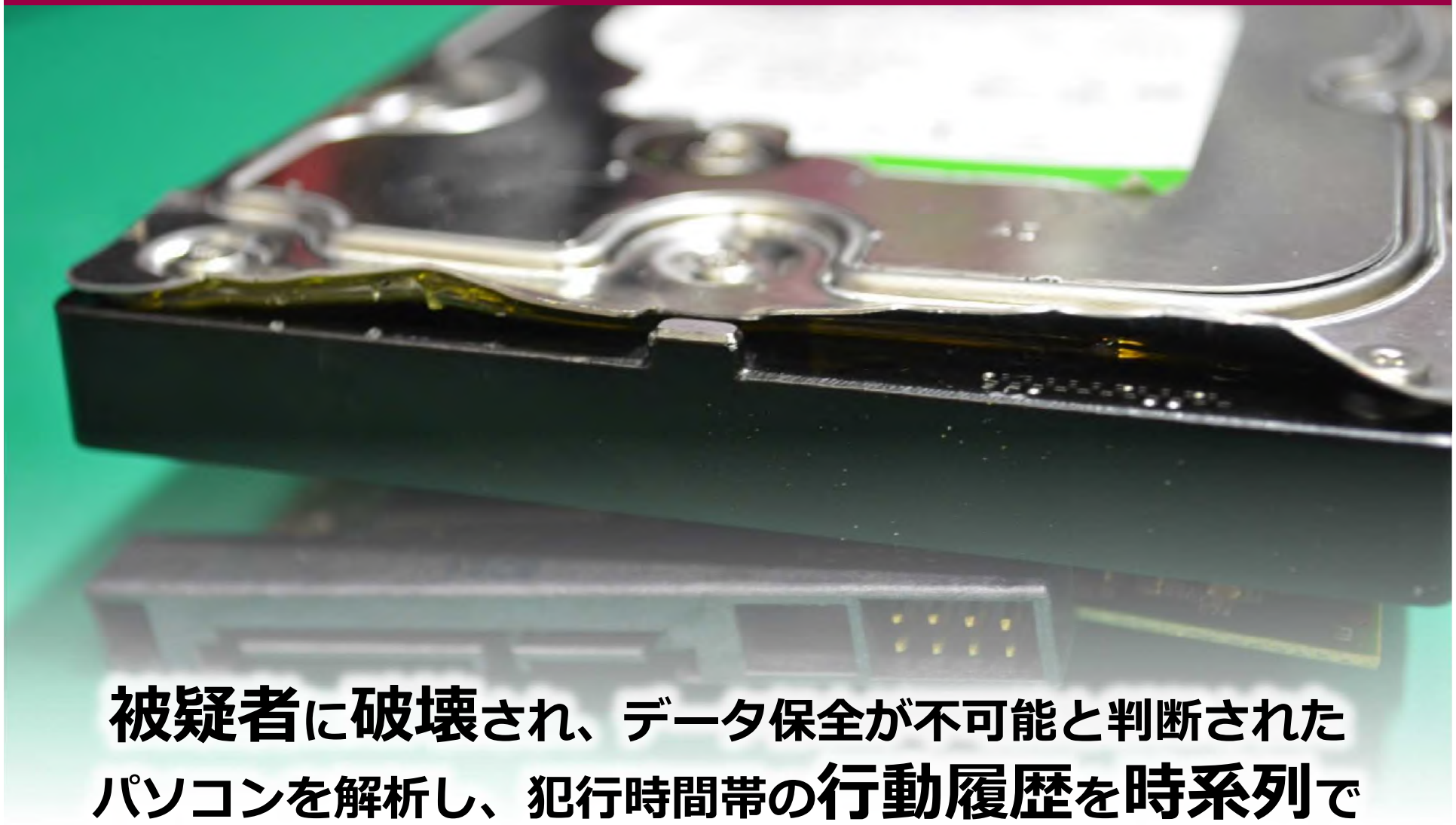
注）この写真のSDカードは、実際の事件証拠品の破壊状況を下垣内太が再現したものです。いずれの写真も本物の証拠品ではございません。

壊れた証拠品からのデータ復旧事例

壊された証拠品からのデータ復旧事例

注）この写真のスマートフォンは、実際の事件証拠品の状態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。

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

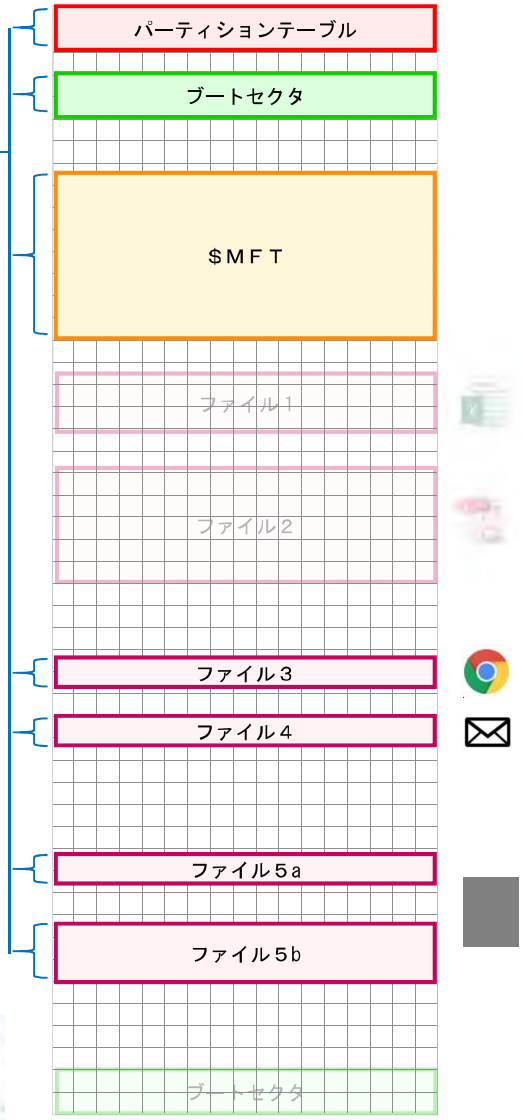
証拠隠滅を狙って破壊されたHDD

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

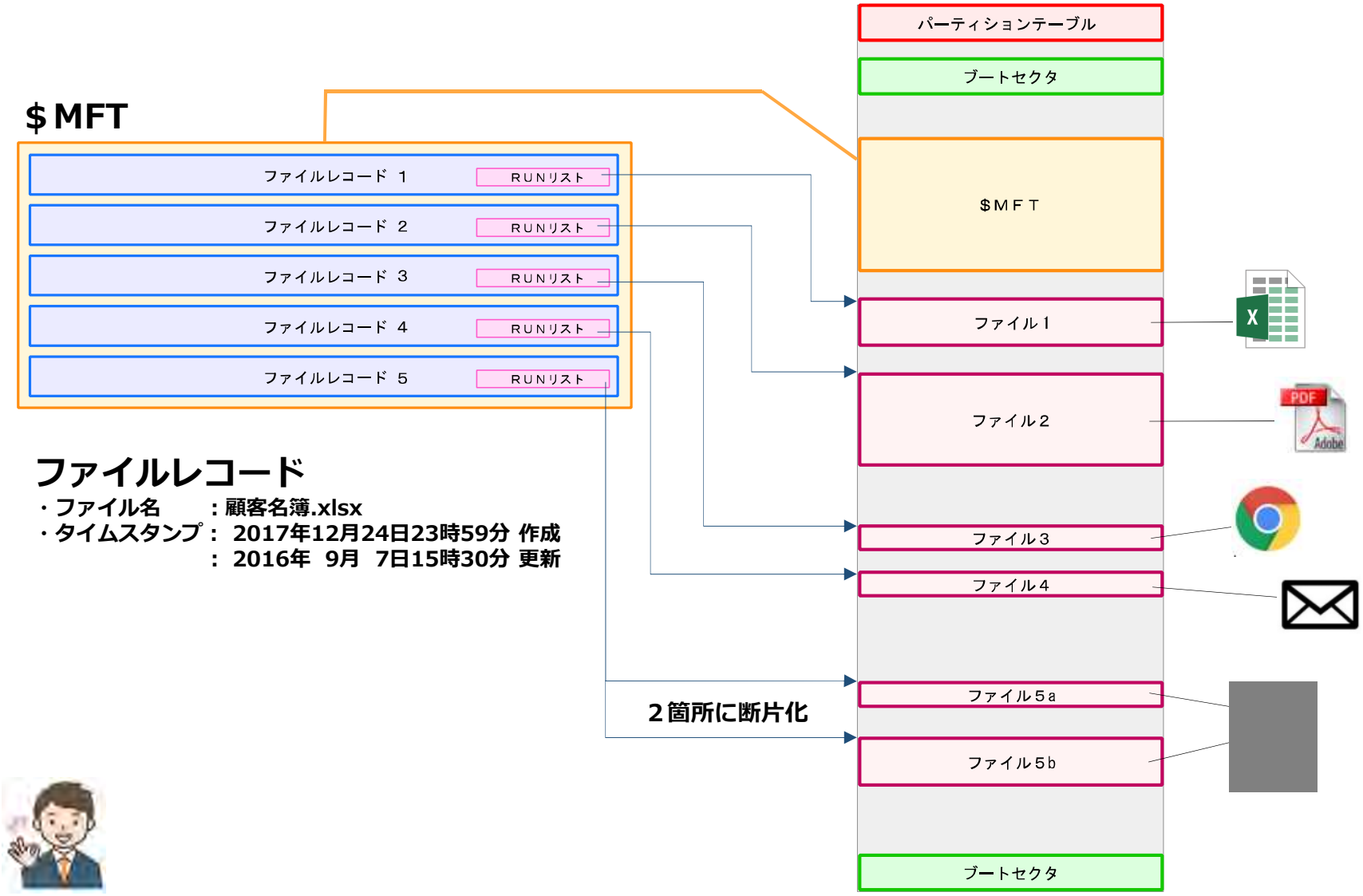
ピンポイントの合計１GB



証拠確保

- ウェブ履歴
- メッセージ
- イベントログ

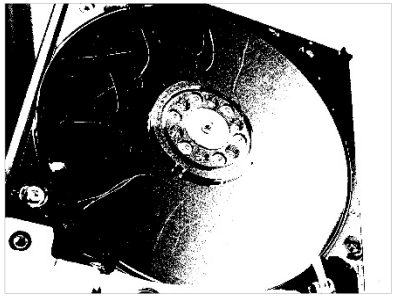
NTFSのデータ配置



ファイルレコード

・ファイル名　　：顧客名簿.xlsx
・タイムスタンプ：2017年12月24日23時59分 作成
　　：2016年 9月 7日15時30分 更新

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

&

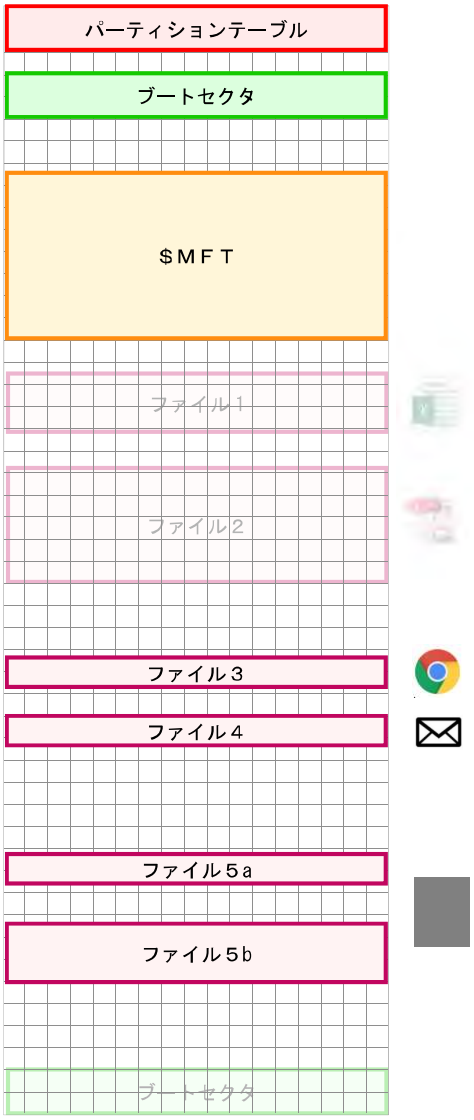
磁気ディスク表層ダメージの低減化

&

部品交換による一時修繕（通常のデータ復旧技術）

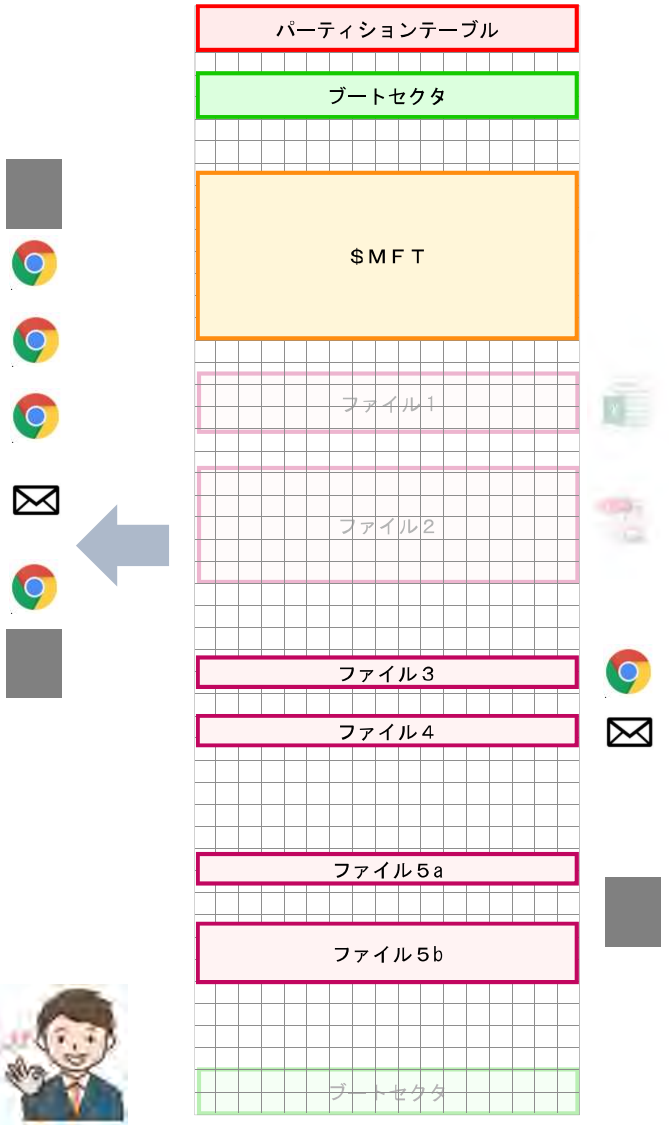
ヘッドアセンブリ交換

制御基板修復



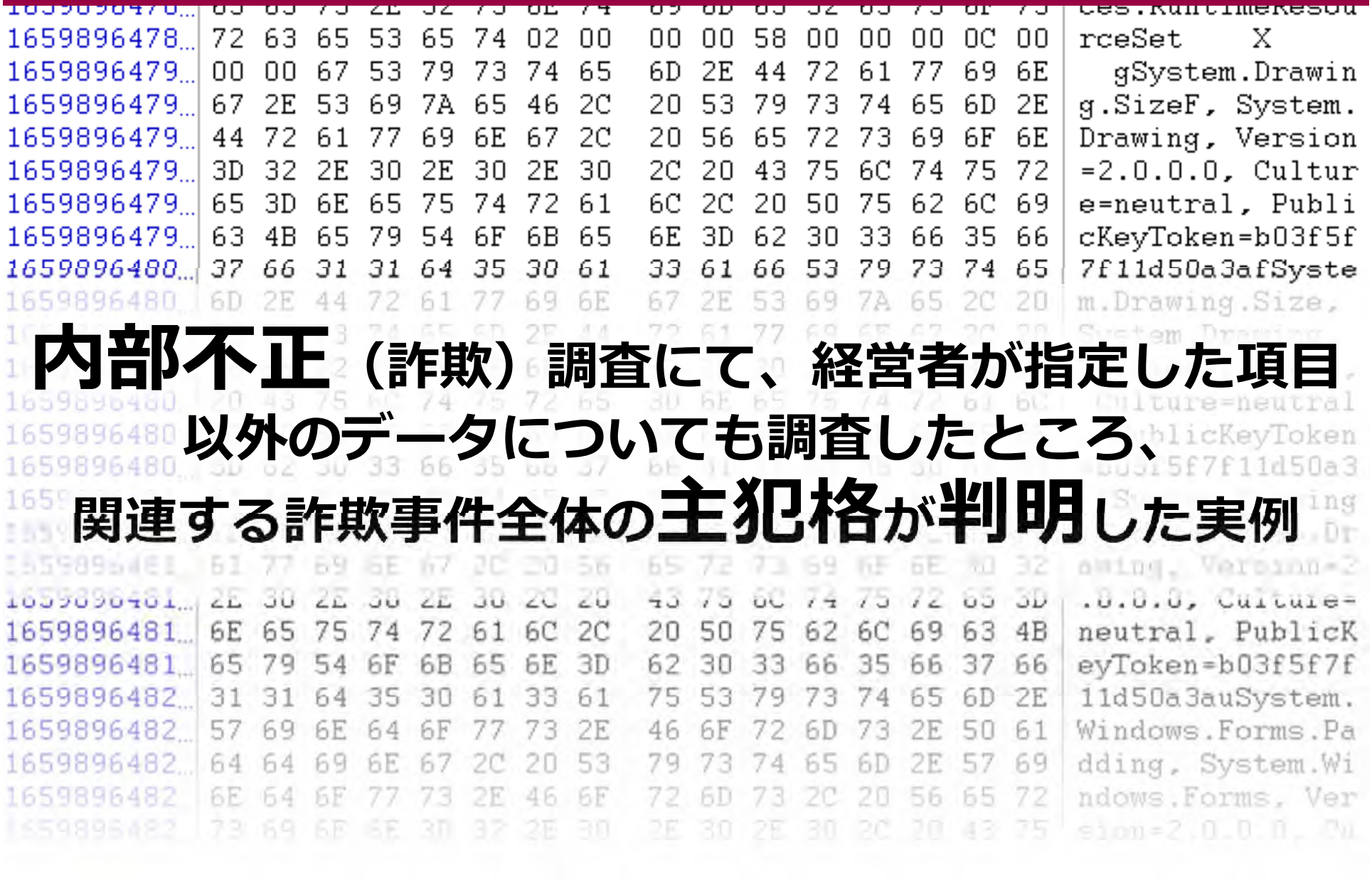
収集したデータを時系列化し、対象者の行動経緯を把握

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

解析対象を特化しすぎると重要証拠を見落とす



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

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？

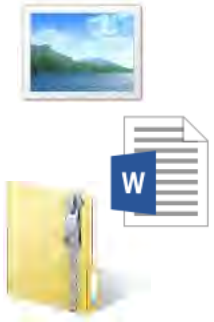
解析後、MS-Wordデータは検出されず。だが、真犯人と未発覚の不正契約が判明。

✕ 解析対象ファイル選択リスト

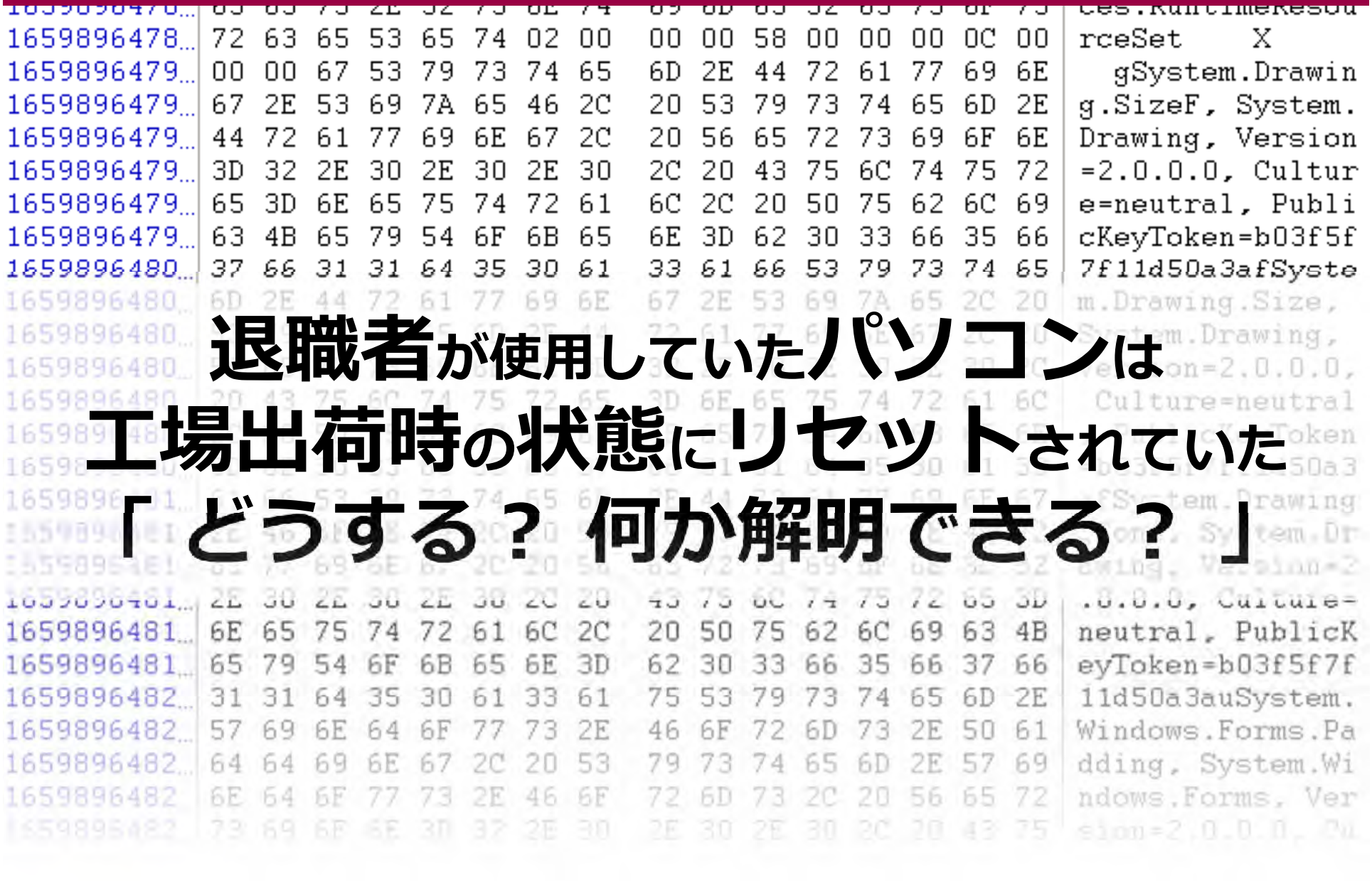
☑ ワード	☐ JPG
☐ エクセル	☐ TIFF
☐ パワーポイント	☐ PST
☐ PDF	☐ EML
☐ BMP	☐ ZIP

◎ 解析対象ファイル選択リスト

☑ ワード	☑ JPG
☑ エクセル	☑ TIFF
☑ パワーポイント	☑ PST
☑ PDF	☑ EML
☑ BMP	☑ ZIP



データ消去済みパソコンに残る証拠



退職者が使用していた**パソコン**は
工場出荷時の**状態**に**リセット**されていた
「どうする？ 何か解明できる？」

工場出荷時の状態にリセットされたパソコンの調査

調査の方向性x2

存在していたデータ

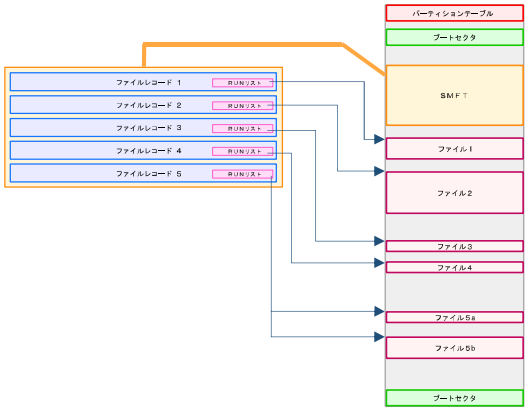
データが消えた経緯

工場出荷時の状態にリセットされたパソコンの調査

調査の方向性 その1

存在していたデータを探す

ファイルシステム解析



残存ファイルレコードの検出とそれに基づくファイルの捜索

ファイルカービング解析

ファイル種別毎に特有のバイナリデータに基づきファイルの存在を検知し種類を識別する方法

アーティファクト解析

- 2019年2月19日 14時20分 Yahoo検索
- 2019年2月19日 14時21分 Yahoo検索
- 2019年2月19日 14時22分 Yahoo検索
- 2019年2月19日 14時23分 Yahoo検索
- 2019年2月19日 14時24分 Yahoo検索
- 2019年2月19日 15時10分 Yahoo検索
- 2019年2月19日 15時20分 Yahoo検索
- 2019年2月19日 15時30分 Yahoo検索
- 2019年2月19日 16時10分 Yahoo検索
- 2019年2月19日 16時11分 Yahoo検索
- 2019年2月19日 20時20分 Yahoo検索
- 2019年2月19日 20時25分 Yahoo検索
- 2019年2月19日 20時33分 Yahoo検索
- 2019年2月19日 20時48分 Yahoo検索

ファイル単位に加え、更に掘り下げてファイルが内包する構成要素も解析

工場出荷時の状態にリセットされたパソコンの調査

調査の方向性 その2

データが消えた経緯を探る

USNジャーナルログ解析

2019年1月19日 14時20分 住所録.xls 削除
2019年1月19日 14時20分 電話帳.xls 削除
2019年1月19日 14時20分 時間割.xls 削除
2019年1月19日 14時20分 分担表.xls 削除
2019年1月19日 14時20分 録画係.xls 削除
2019年1月19日 14時20分 論文A.doc 削除
2019年1月19日 14時20分 論文B.xls 削除
2019年1月19日 14時20分 phone.xls 削除
2019年1月19日 16時10分 DCM723.jpg 作成
2019年1月19日 16時11分 DCM724.jpg 作成
2019年1月19日 20時20分 DCM725.jpg 作成
2019年1月19日 20時25分 連絡表.xls 更新
2019年1月19日 20時33分 回覧板.xls 更新
2019年1月19日 20時48分 朝当番.xls 削除

ファイルの作成・更新や削除履歴（ファイル名や時刻）の解明

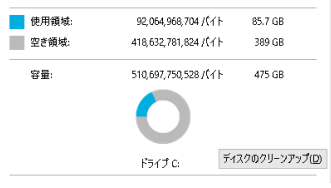
OSセットアップ経緯解析

パーティション初期化日時
1．誰かがPCを操作した
2．初期化が行われた
3．初期化実施の日時
4．OSインストール作業の始まり

OSインストール日時
1．OSセットアップ日時
2．コンピュータ名・ユーザ名
3．ユーザアカウント追加日時
4．誰かがPCを操作した

OSセットアップ時に、パーティションの初期化を行ったか否か、処理が開始された時刻などの解明

空き領域のHEX値解析



この領域↓

この領域↓

空き領域の毎バイトHEX値（16進数）の出現率を算出。均一の場合、**乱数書き込み消去実施の可能性が浮上**

毎バイトHEX値の出現率解析

空き領域のバイナリを目視チェック

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
C93C58D600	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D610	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D620	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D630	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D640	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D650	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D660	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D670	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D680	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D690	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D700	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D710	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D720	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D730	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D740	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D750	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D760	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D770	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D780	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D790	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

同じ値（x00）の連続 ≒ 何もないなぁ

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
03AFAC00	AC	C4	6C	18	4B	56	85	F4	5F	54	C9	8E	E7	0B	4C	5D
03AFAC10	04	ED	27	72	C3	2B	C3	BB	38	FC	3F	C7	45	1D	ED	67
03AFAC20	B3	A6	8B	97	89	05	C6	23	56	4F	59	69	32	51	CC	65
03AFAC30	39	EB	8F	7D	84	51	A3	79	C3	5B	F6	70	AA	A0	10	13
03AFAC40	C8	90	D8	9A	98	24	07	DD	63	25	B3	F5	BC	D1	CD	20
03AFAC50	53	B1	BB	AD	77	85	BF	42	51	50	93	3A	C5	AF	9B	62
03AFAC60	48	88	03	A1	52	00	97	58	3A	3C	8A	30	A0	F6	C2	1F
03AFAC70	18	87	E8	06	A5	73	0F	56	DD	5C	2B	A4	0D	DB	C1	9E
03AFAC80	91	8E	C7	52	0E	78	69	C8	D0	12	39	6A	0E	FC	10	D6
03AFAC90	E9	3C	35	F2	95	CE	8B	4D	D5	E3	46	B5	8A	C6	33	BF
03AFACA0	DA	CF	02	16	77	D5	E2	8B	09	27	A1	6A	64	51	4E	C6
03AFACB0	E2	C9	C6	97	F8	24	69	22	A7	00	31	92	5C	32	93	74
03AFACC0	72	4E	F3	56	17	AB	8D	65	0A	94	EF	23	49	25	25	3D
03AFACD0	3A	41	73	FC	44	60	BA	7F	15	32	F0	6F	92	A6	5E	05
03AFACE0	92	02	13	0A	64	9E	EC	FB	3B	3A	8B	4D	5A	54	6A	50
03AFACF0	F1	E8	DC	DF	A8	A3	00	42	B2	7A	9F	D1	70	48	0E	B7
03AFAD00	63	45	AC	70	58	B5	22	61	19	9F	A1	32	5D	18	8C	9A
03AFAD10	6F	38	E4	7C	0E	2B	87	94	EE	3F	6D	EC	82	1A	41	02
03AFAD20	13	FB	29	D6	54	FF	CA	4D	4B	C2	72	7A	E5	0D	50	FD
03AFAD30	F9	E9	29	90	7E	F4	32	86	52	28	A3	31	56	F2	3C	F6
03AFAD40	54	4F	5A	38	92	1F	00	E5	7B	C4	D8	1A	19	7C	53	89
03AFAD50	6E	DE	FD	B9	CD	59	45	6B	17	4F	18	B8	EC	81	D7	A5
03AFAD60	53	CD	CE	B5	A0	81	E2	61	E6	F5	81	E1	02	35	91	36
03AFAD70	08	BE	7F	85	95	37	E2	24	0D	29	82	D9	17	DD	84	09
03AFAD80	57	3C	0A	8F	83	53	F0	E1	72	FB	72	40	72	F8	54	D2
03AFAD90	DE	68	9B	50	85	00	11	BA	79	C3	E7	33	D4	46	F3	22
03AFADA0	D7	B5	E3	0B	96	DB	52	96	51	FF	2E	30	76	CD	9A	DB
03AFADB0	97	D2	D6	A4	F7	32	AA	6C	65	86	1A	F3	CA	F2	06	F4
03AFADC0	94	6C	74	19	5B	34	1C	41	C7	B3	48	C2	9A	B9	7E	7D
03AFADD0	76	6C	AB	16	93	24	78	33	F8	90	B1	0D	2D	98	DE	54
03AFADE0	F1	59	B7	63	B0	AE	8D	D1	84	65	E5	3A	CD	FF	0D	13
03AFADF0	68	C7	6F	B9	39	FD	F3	CE	86	1B	62	C5	99	B0	80	5F

お！ 削除済みファイル復元できるかも！

毎バイトHEX値の出現率解析

空き領域のバイナリを目視チェック

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
C93C58D600	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D610	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D620	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D630	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D640	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D650	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D660	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D670	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D680	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D690	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D6F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D700	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D710	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D720	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D730	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D740	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D750	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D760	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D770	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D780	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D790	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
C93C58D7F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

もしかして、空き領域すべてx00 ？

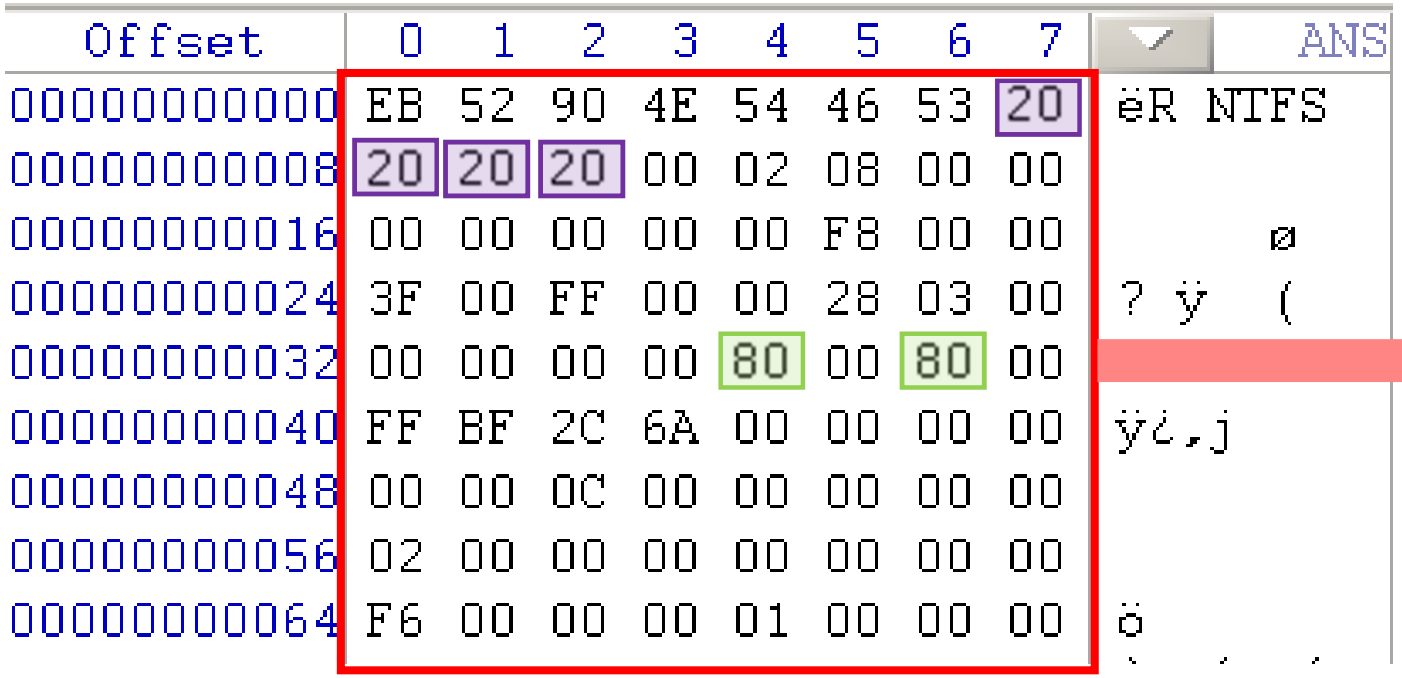
なんとなく違和感を感じることがある、、、

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
03AFAC00	AC	C4	6C	18	4B	56	85	F4	5F	54	C9	8E	E7	0B	4C	5D
03AFAC10	04	ED	27	72	C3	2B	C3	BB	38	FC	3F	C7	45	1D	ED	67
03AFAC20	B3	A6	8B	97	89	05	C6	23	56	4F	59	69	32	51	CC	65
03AFAC30	39	EB	8F	7D	84	51	A3	79	C3	5B	F6	70	AA	A0	10	13
03AFAC40	C8	90	D8	9A	98	24	07	DD	63	25	B3	F5	BC	D1	CD	20
03AFAC50	53	B1	BB	AD	77	85	BF	42	51	50	93	3A	C5	AF	9B	62
03AFAC60	48	88	03	A1	52	00	97	58	3A	3C	8A	30	A0	F6	C2	1F
03AFAC70	18	87	E8	06	A5	73	0F	56	DD	5C	2B	A4	0D	DB	C1	9E
03AFAC80	91	8E	C7	52	0E	78	69	C8	D0	12	39	6A	0E	FC	10	D6
03AFAC90	E9	3C	35	F2	95	CE	8B	4D	D5	E3	46	B5	8A	C6	33	BF
03AFACA0	DA	CF	02	16	77	D5	E2	8B	09	27	A1	6A	64	51	4E	C6
03AFACB0	E2	C9	C6	97	F8	24	69	22	A7	00	31	92	5C	32	93	74
03AFACC0	72	4E	F3	56	17	AB	8D	65	0A	94	EF	23	49	25	25	3D
03AFACD0	3A	41	73	FC	44	60	BA	7F	15	32	F0	6F	92	A6	5E	05
03AFAD10	6F	38	E4	7C	0E	2B	87	94	EE	3F	6D	EC	82	1A	41	02
03AFAD20	13	FB	29	D6	54	FF	CA	4D	4B	C2	72	7A	E5	0D	50	FD
03AFAD30	F9	E9	29	90	7E	F4	32	86	52	28	A3	31	56	F2	3C	F6
03AFAD40	54	4F	5A	38	92	1F	00	E5	7B	C4	D8	1A	19	7C	53	89
03AFAD50	6E	DE	FD	B9	CD	59	45	6B	17	4F	18	B8	EC	81	D7	A5
03AFAD60	53	CD	CE	B5	A0	81	E2	61	E6	F5	81	E1	02	35	91	36
03AFAD70	08	BE	7F	85	95	37	E2	24	0D	29	82	D9	17	DD	84	09
03AFAD80	57	3C	0A	8F	83	53	F0	E1	72	FB	72	40	72	F8	54	D2
03AFAD90	DE	68	9B	50	85	00	11	BA	79	C3	E7	33	D4	46	F3	22
03AFADA0	D7	B5	E3	0B	96	DB	52	96	51	FF	2E	30	76	CD	9A	DB
03AFADB0	97	D2	D6	A4	F7	32	AA	6C	65	86	1A	F3	CA	F2	06	F4
03AFADC0	94	6C	74	19	5B	34	1C	41	C7	B3	48	C2	9A	B9	7E	7D
03AFADD0	76	6C	AB	16	93	24	78	33	F8	90	B1	0D	2D	98	DE	54
03AFADE0	F1	59	B7	63	B0	AE	8D	D1	84	65	E5	3A	CD	FF	0D	13
03AFADF0	68	C7	6F	B9	39	FD	F3	CE	86	1B	62	C5	99	B0	80	5F

x00の連続領域が無い、、なんか変、、

毎バイトHEX値の出現率解析

毎バイトHEX値（16進数）の出現数と出現率



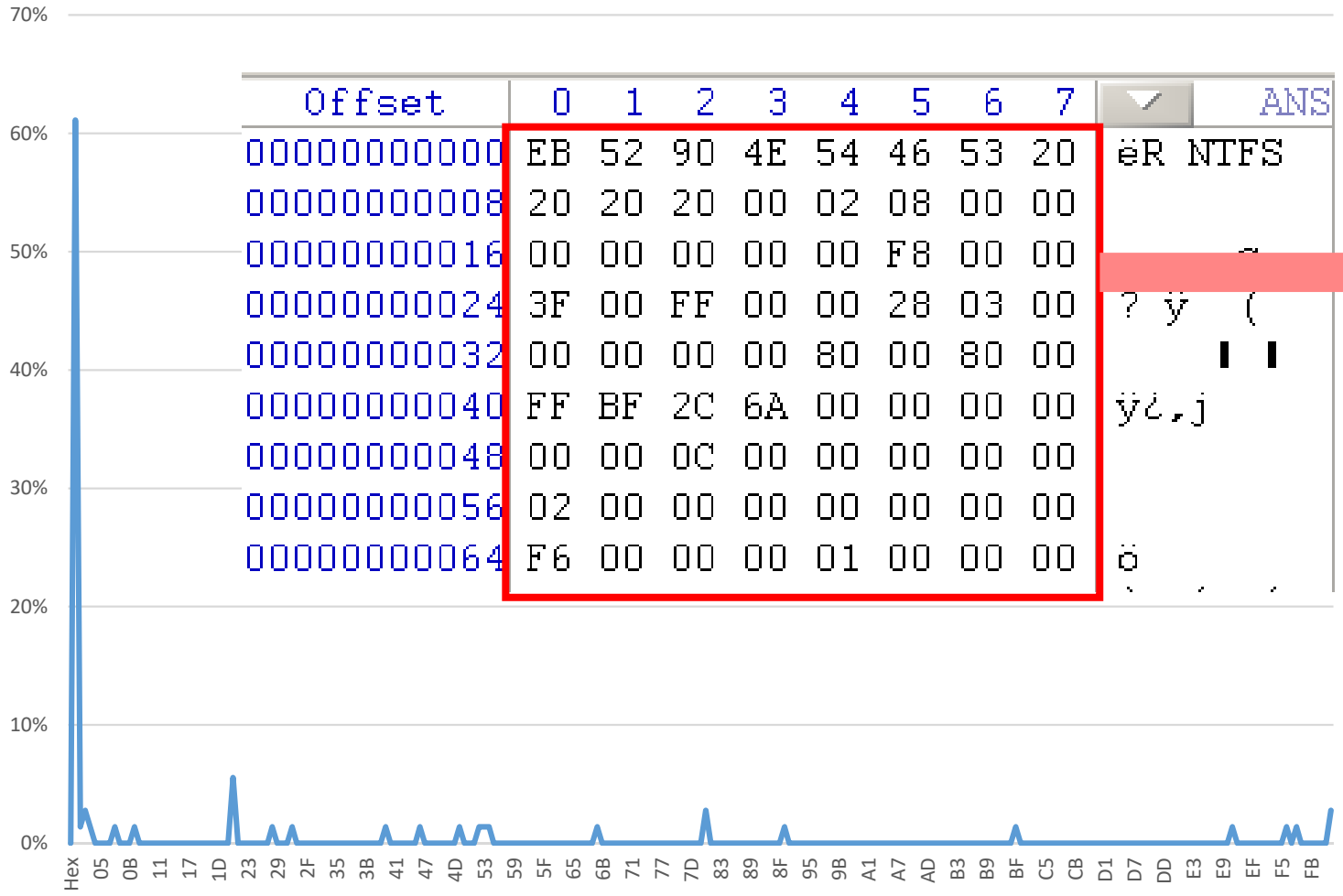
Offset	0	1	2	3	4	5	6	7	ANS
00000000000	EB	52	90	4E	54	46	53	20	ëR NTFS
00000000008	20	20	20	00	02	08	00	00	
00000000016	00	00	00	00	00	F8	00	00	ø
00000000024	3F	00	FF	00	00	28	03	00	? ÿ (
00000000032	00	00	00	00	80	00	80	00	
00000000040	FF	BF	2C	6A	00	00	00	00	ÿ¿,j
00000000048	00	00	0C	00	00	00	00	00	
00000000056	02	00	00	00	00	00	00	00	
00000000064	F6	00	00	00	01	00	00	00	ö

X-WaysのAnalyze Block(Disk)機能で計算可

Hex	No	%
00	44	61.11%
20	4	5.56%
02	2	2.78%
80	2	2.78%
FF	2	2.78%
01	1	1.39%
03	1	1.39%
08	1	1.39%
0C	1	1.39%
28	1	1.39%
2C	1	1.39%
3F	1	1.39%
46	1	1.39%
4E	1	1.39%
52	1	1.39%
53	1	1.39%
54	1	1.39%
6A	1	1.39%
90	1	1.39%
BF	1	1.39%
EB	1	1.39%
F6	1	1.39%
F8	1	1.39%

毎バイトHEX値の出現率解析

毎バイトHEX値（16進数）の出現率

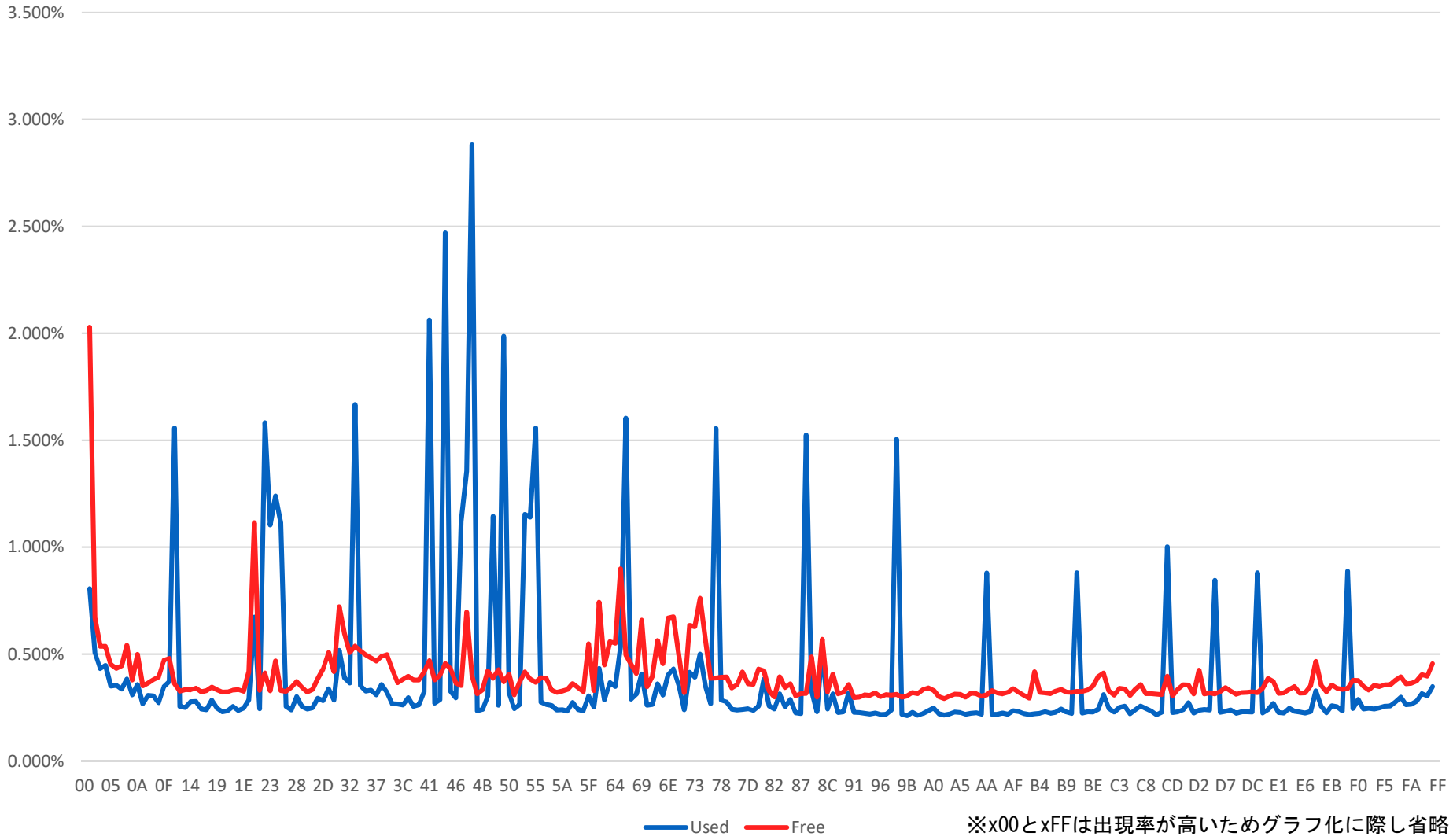


Offset	0	1	2	3	4	5	6	7	ANS
00000000000	EB	52	90	4E	54	46	53	20	ëR NTFS
00000000008	20	20	20	00	02	08	00	00	
00000000016	00	00	00	00	00	F8	00	00	ø
00000000024	3F	00	FF	00	00	28	03	00	? ÿ (
00000000032	00	00	00	00	80	00	80	00	▌ ▌
00000000040	FF	BF	2C	6A	00	00	00	00	ÿ¿,j
00000000048	00	00	0C	00	00	00	00	00	
00000000056	02	00	00	00	00	00	00	00	
00000000064	F6	00	00	00	01	00	00	00	ö

Hex	%
00	61.11%
01	1.39%
02	2.78%
03	1.39%
04	0.00%
05	0.00%
06	0.00%
07	0.00%
08	1.39%
09	0.00%
0A	0.00%
0B	0.00%
0C	1.39%
0D	0.00%
0E	0.00%
0F	0.00%
10	0.00%
11	0.00%
12	0.00%
13	0.00%
14	0.00%
15	0.00%
16	0.00%

使用領域と空き領域の毎バイトHEX値出現率比較

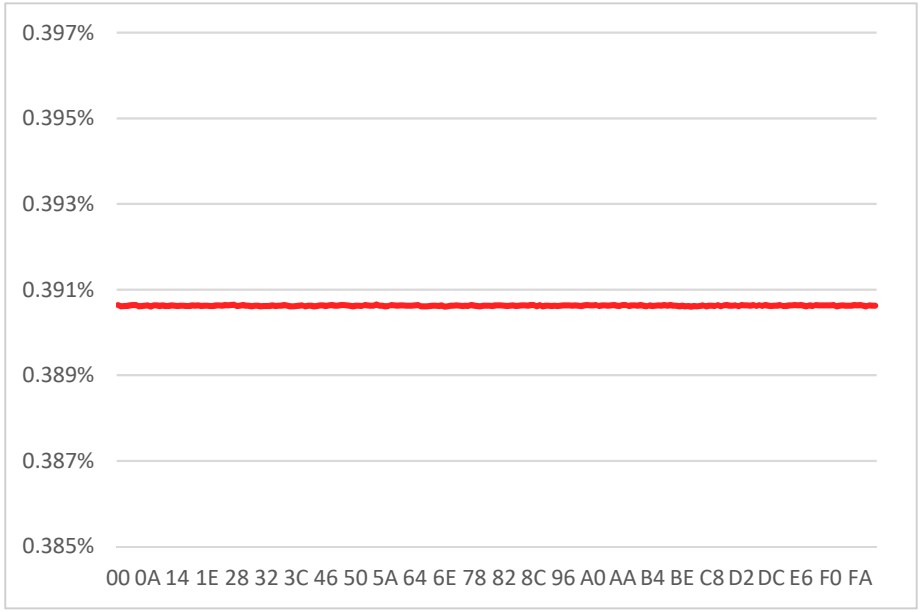
一般的な使用状態のPCの場合



※x00とxFFは出現率が高いためグラフ化に際し省略

毎バイトHEX値の出現率解析

空き領域の毎バイトHEX値の出現率をグラフ化



HEX値の出現率が均一

↓

乱数？

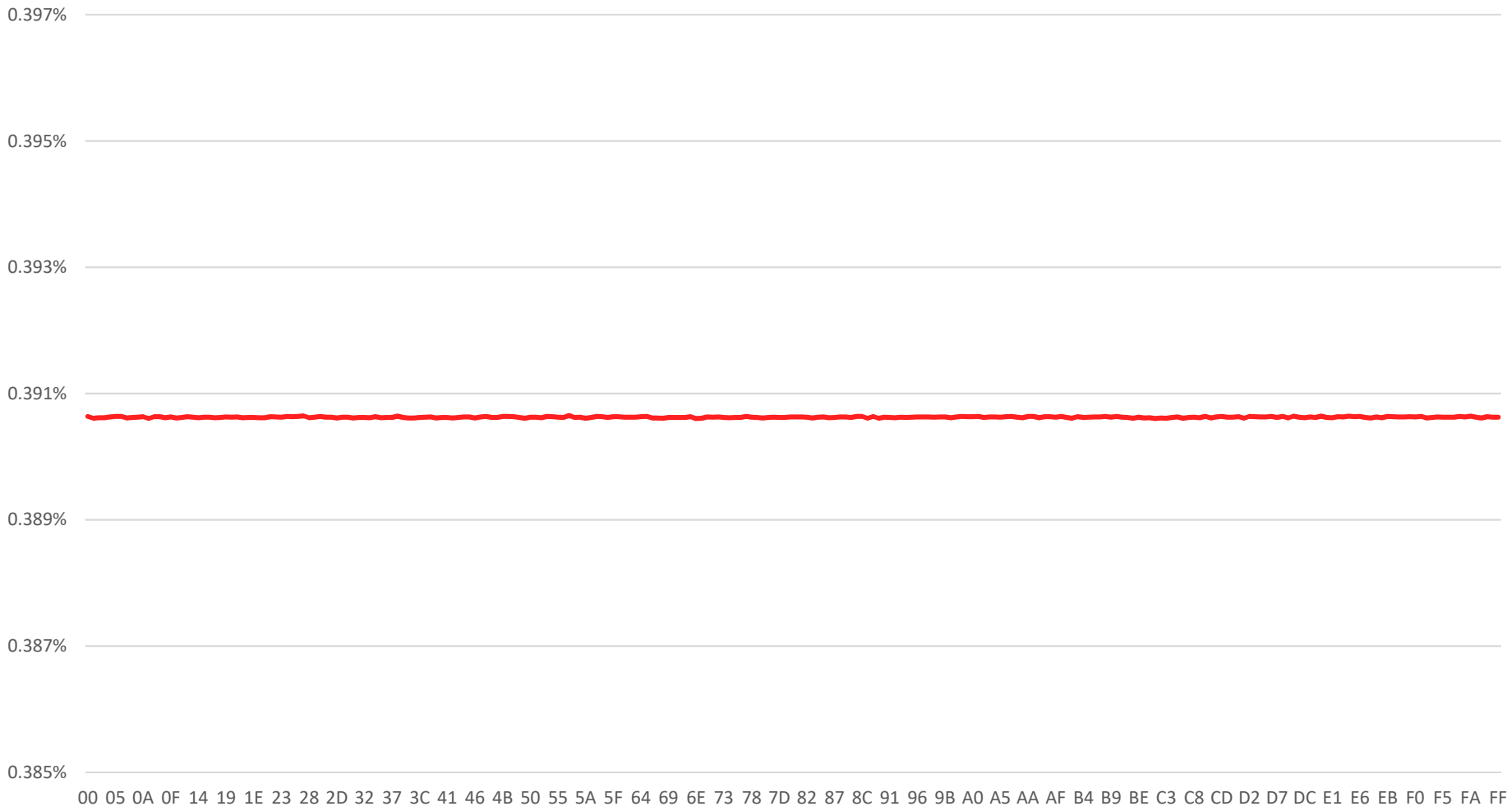
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
03AFAC00	AC	C4	6C	18	4B	56	85	F4	5F	54	C9	8E	E7	0B	4C	5D
03AFAC10	04	ED	27	72	C3	2B	C3	BB	38	FC	3F	C7	45	1D	ED	67
03AFAC20	B3	A6	8B	97	89	05	C6	23	56	4F	59	69	32	51	CC	65
03AFAC30	39	EB	8F	7D	84	51	A3	79	C3	5B	F6	70	AA	A0	10	13
03AFAC40	C8	90	D8	9A	98	24	07	DD	63	25	B3	F5	BC	D1	CD	20
03AFAC50	53	B1	BB	AD	77	85	BF	42	51	50	93	3A	C5	AF	9B	62
03AFAC60	48	88	03	A1	52	00	97	58	3A	3C	8A	30	A0	F6	C2	1F
03AFAC70	18	87	E8	06	A5	73	0F	56	DD	5C	2B	A4	0D	DB	C1	9E
03AFAC80	91	8E	C7	52	0E	78	69	C8	D0	12	39	6A	0E	FC	10	D6
03AFAC90	E9	3C	35	F2	95	CE	8B	4D	D5	E3	46	B5	8A	C6	33	BF
03AFACA0	DA	CF	02	16	77	D5	E2	8B	09	27	A1	6A	64	51	4E	C6
03AFACB0	E2	C9	C6	97	F8	24	69	22	A7	00	31	92	5C	32	93	74
03AFACC0	72	4E	F3	56	17	AB	8D	65	0A	94	EF	23	49	25	25	3D
03AFACD0	3A	41	73	FC	44	60	BA	7F	15	32	F0	6F	92	A6	5E	05
03AFACE0	92	02	13	0A	64	9E	EC	FB	3B	3A	8B	4D	5A	54	6A	50
03AFACF0	F1	E8	DC	DF	A8	A3	00	42	B2	7A	9F	D1	70	48	0E	B7
03AFAD00	63	45	AC	70	58	B5	22	61	19	9F	A1	32	5D	18	8C	9A
03AFAD10	6F	38	E4	7C	0E	2B	87	94	EE	3F	6D	EC	82	1A	41	02
03AFAD20	13	FB	29	D6	54	FF	CA	4D	4B	C2	72	7A	E5	0D	50	FD
03AFAD30	F9	E9	29	90	7E	F4	32	86	52	28	A3	31	56	F2	3C	F6
03AFAD40	54	4F	5A	38	92	1F	00	E5	7B	C4	D8	1A	19	7C	53	89
03AFAD50	6E	DE	FD	B9	CD	59	45	6B	17	4F	18	B8	EC	81	D7	A5
03AFAD60	53	CD	CE	B5	A0	81	E2	61	E6	F5	81	E1	02	35	91	36
03AFAD70	08	BE	7F	85	95	37	E2	24	0D	29	82	D9	17	DD	84	09
03AFAD80	57	3C	0A	8F	83	53	F0	E1	72	FB	72	40	72	F8	54	D2
03AFAD90	DE	68	9B	50	85	00	11	BA	79	C3	E7	33	D4	46	F3	22
03AFADA0	D7	B5	E3	0B	96	DB	52	96	51	FF	2E	30	76	CD	9A	DB
03AFADB0	97	D2	D6	A4	F7	32	AA	6C	65	86	1A	F3	CA	F2	06	F4
03AFADC0	94	6C	74	19	5B	34	1C	41	C7	B3	48	C2	9A	B9	7E	7D
03AFADD0	76	6C	AB	16	93	24	78	33	F8	90	B1	0D	2D	98	DE	54
03AFADE0	F1	59	B7	63	B0	AE	8D	D1	84	65	E5	3A	CD	FF	0D	13
03AFADF0	68	C7	6F	B9	39	FD	F3	CE	86	1B	62	C5	99	B0	80	5F

x00の連続領域が無い、、なんか変、、

使用領域と空き領域の毎バイトHEX値出現率比較

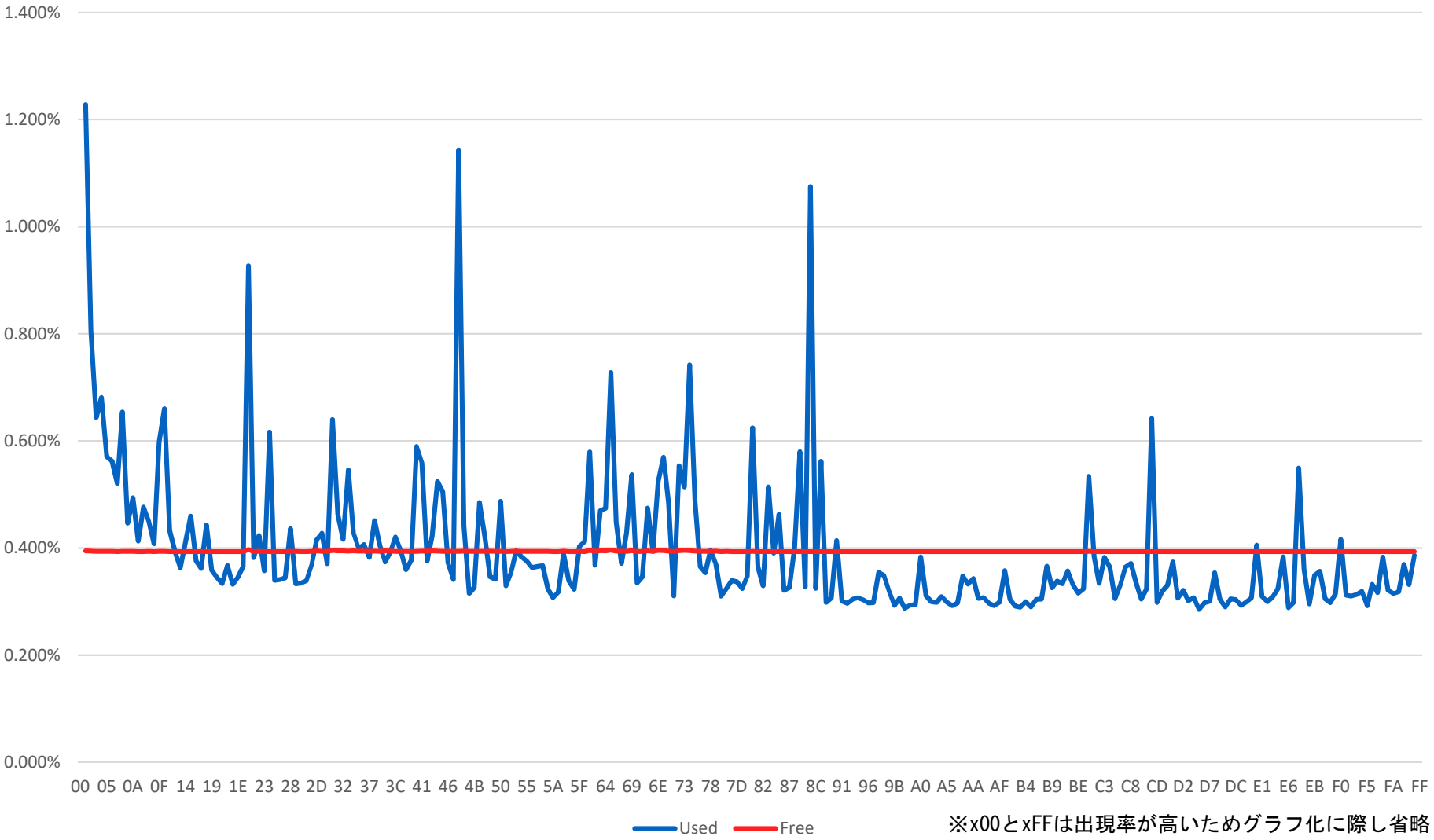
cipher.exe /w コマンド処理後の空き領域

↑空き領域に「x00」「xFF」「乱数」を書き込む処理



使用領域と空き領域の毎バイトHEX値出現率比較

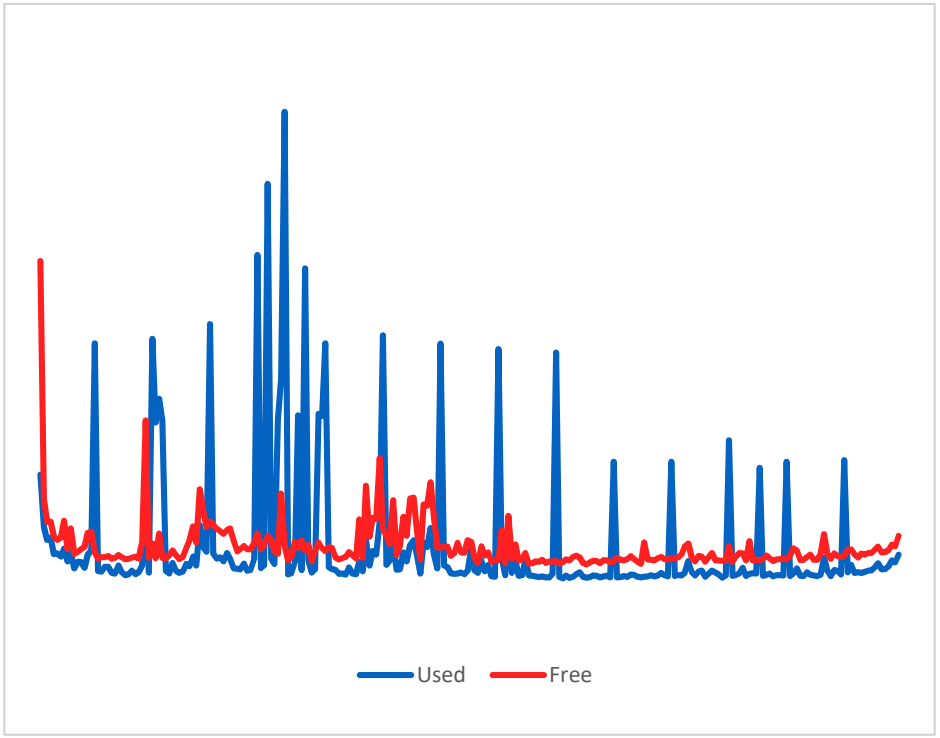
空き領域が乱数書き込み消去されたと考えられるPC



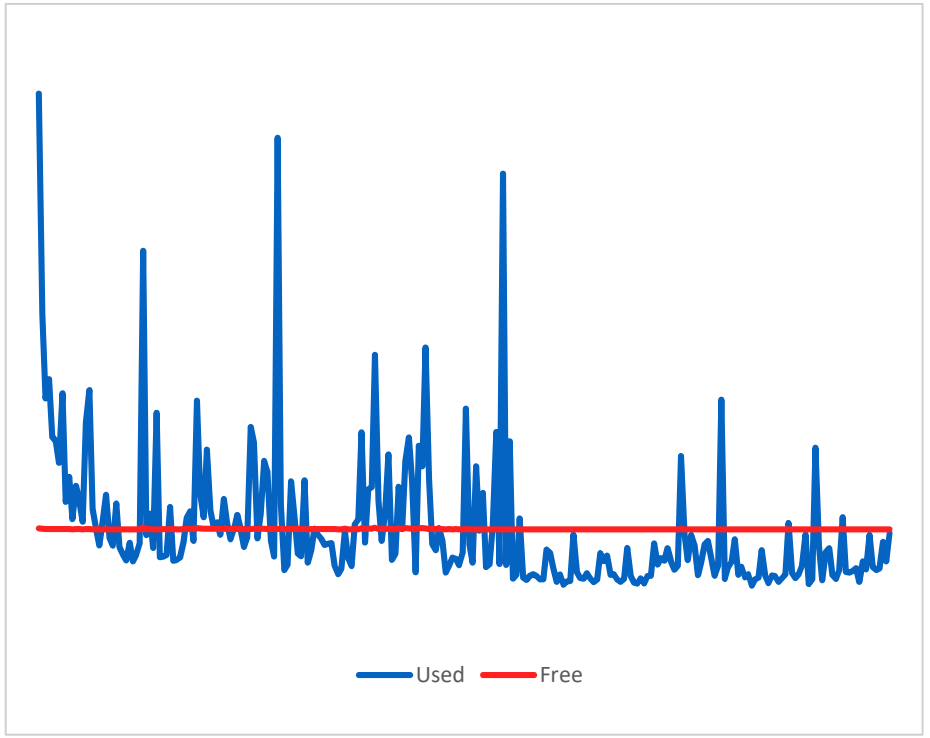
※x00とxFFは出現率が高いためグラフ化に際し省略

使用領域と空き領域の毎バイトHEX値出現率比較

空き領域のHEX値出現値に浮かび上がるデータ消去方式



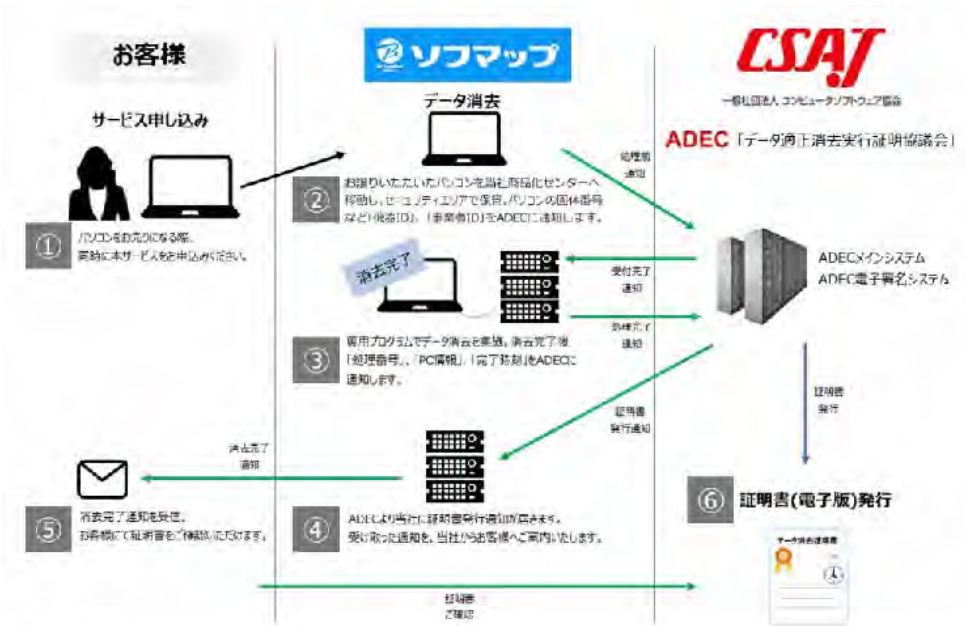
一般的な使われた状態のPC



乱数書き込み消去されたPC

データを消すことへの**強い意思**の表れか

CSAJ - ADEC：データ適正消去 第三者証明サービス



データ消去証明書(サンプル)

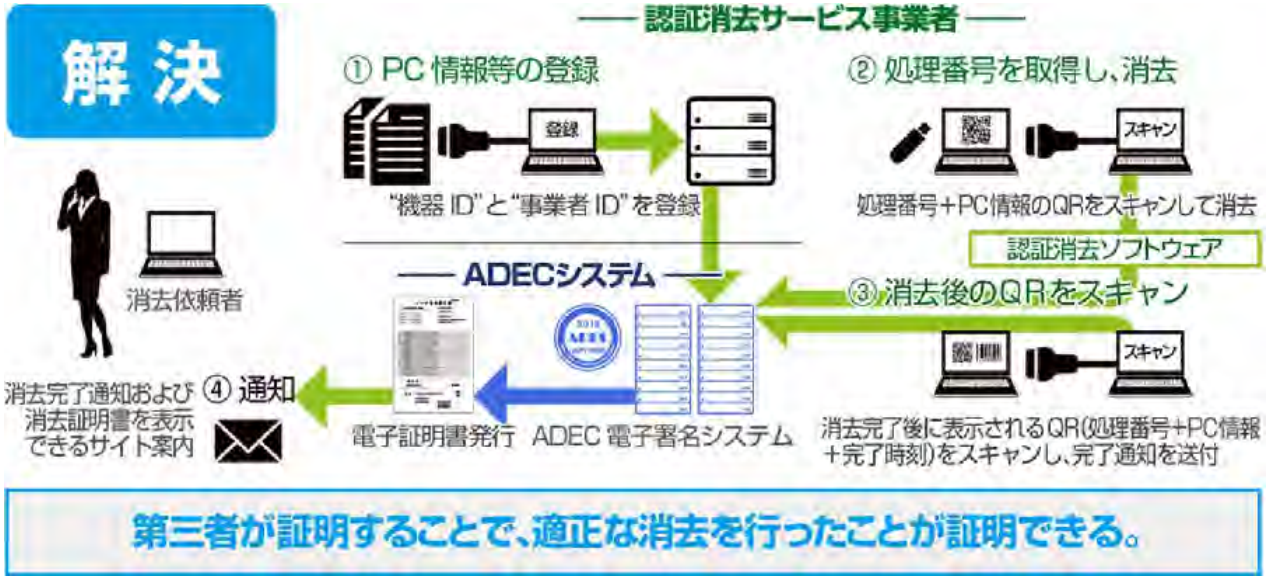
データ適正消去実行証明書
ADEC発行

データ消去証明書（ソフト消去）
ソフマップ発行

データ消去証明書(物理破壊)
ソフマップ発行

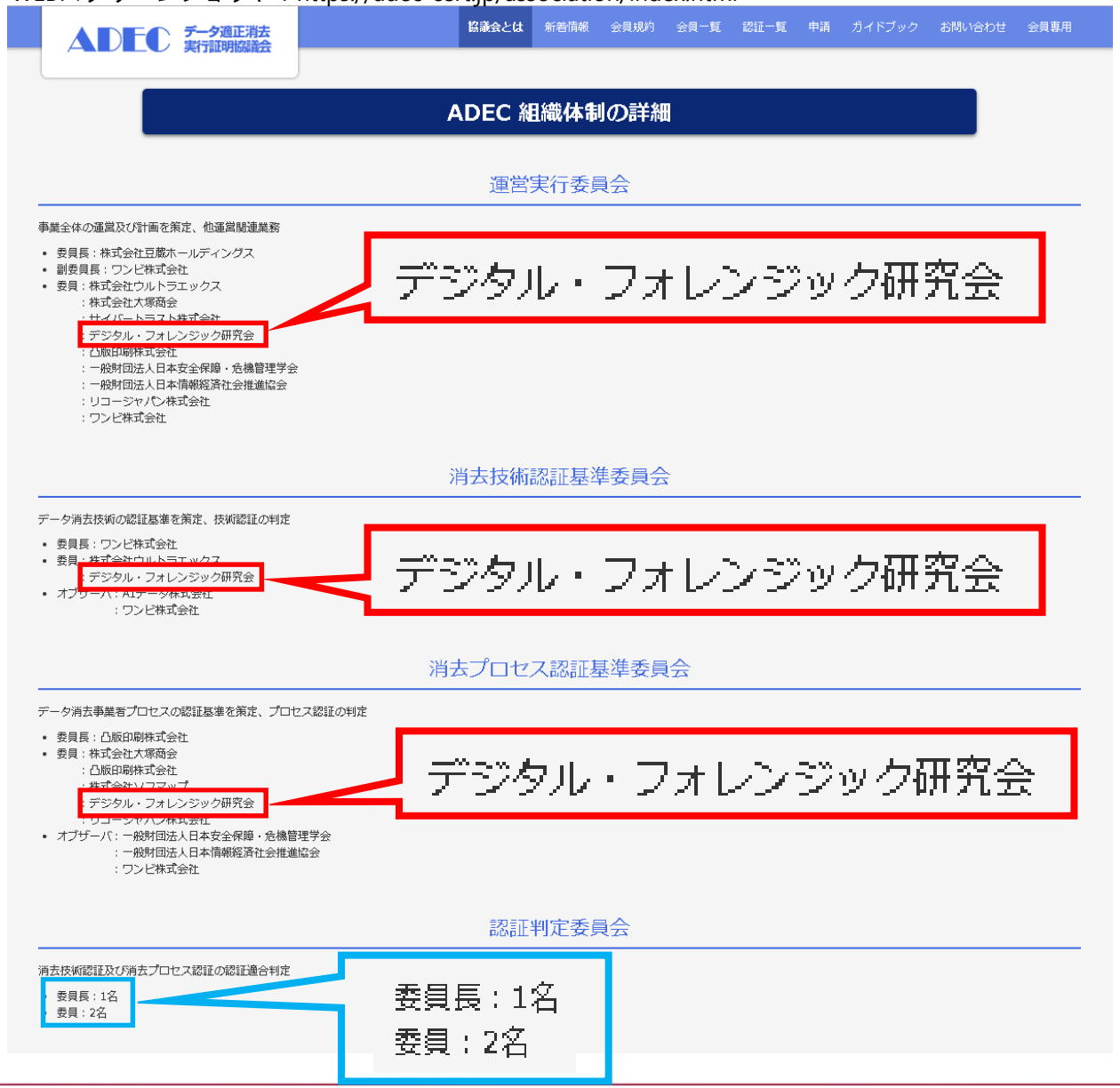
https://www.sofmap.com/contents/?id=erase-data&sid=certificate-service#link_1

CSAJ - ADEC：データ適正消去 第三者証明サービス



ADEC と IDF の関係

WEBスクリーンショット：https://adec-cert.jp/association/index.html



IDFはADECの運営をサポート

・運営実行委員会
・消去技術認証基準委員会
・消去プロセス認証委員会

上記3委員会は、沼田 理 氏がIDFとして参与

※沼田理氏は、データ消去分科会メンバー

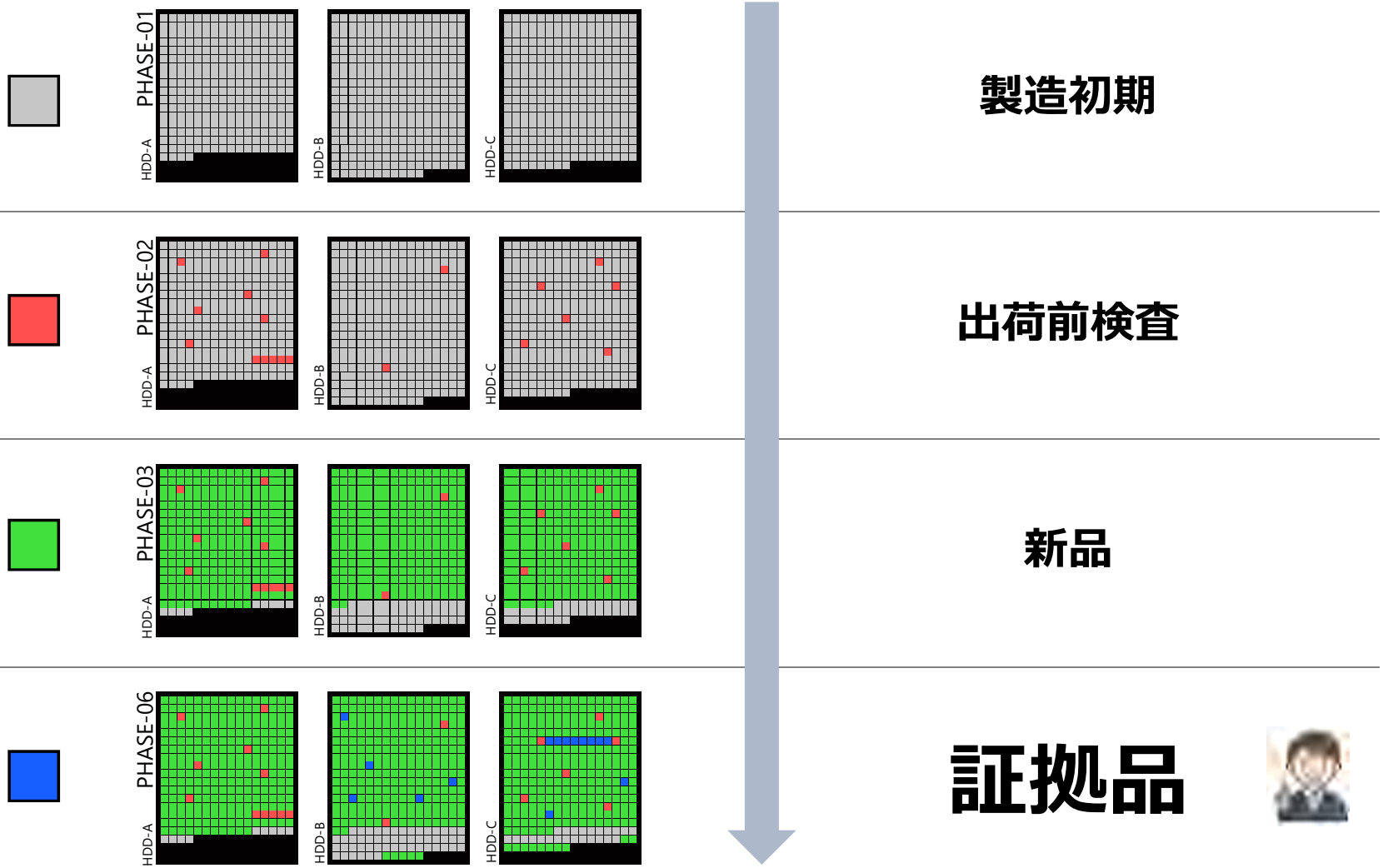
認証判定委員会は、IDF理事である佐々木 良一 教授と手塚 悟 教授が委員長と委員として参与

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

HDD - 物理セクタと論理セクタの構造



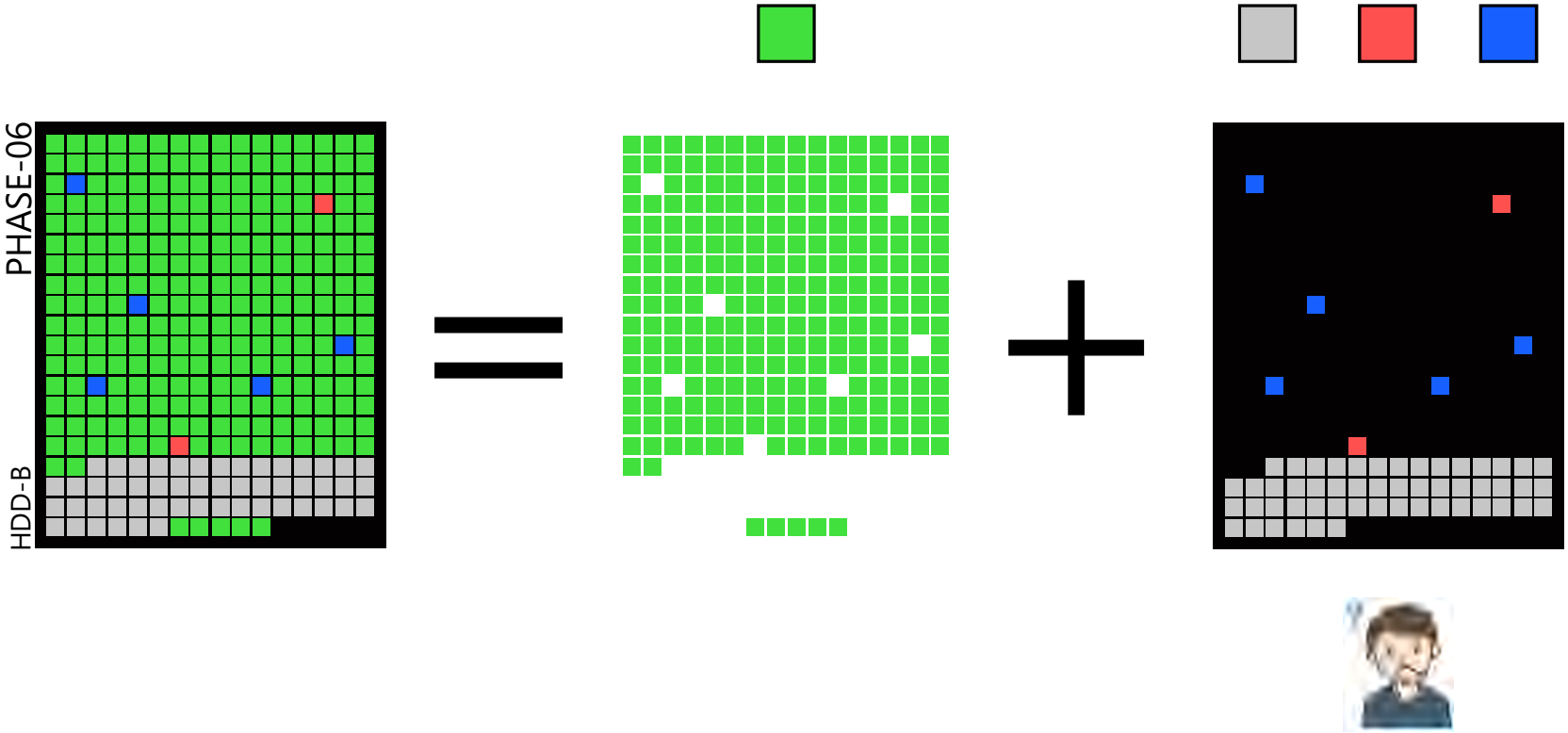
LBAが割り当てられていないセクタ

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

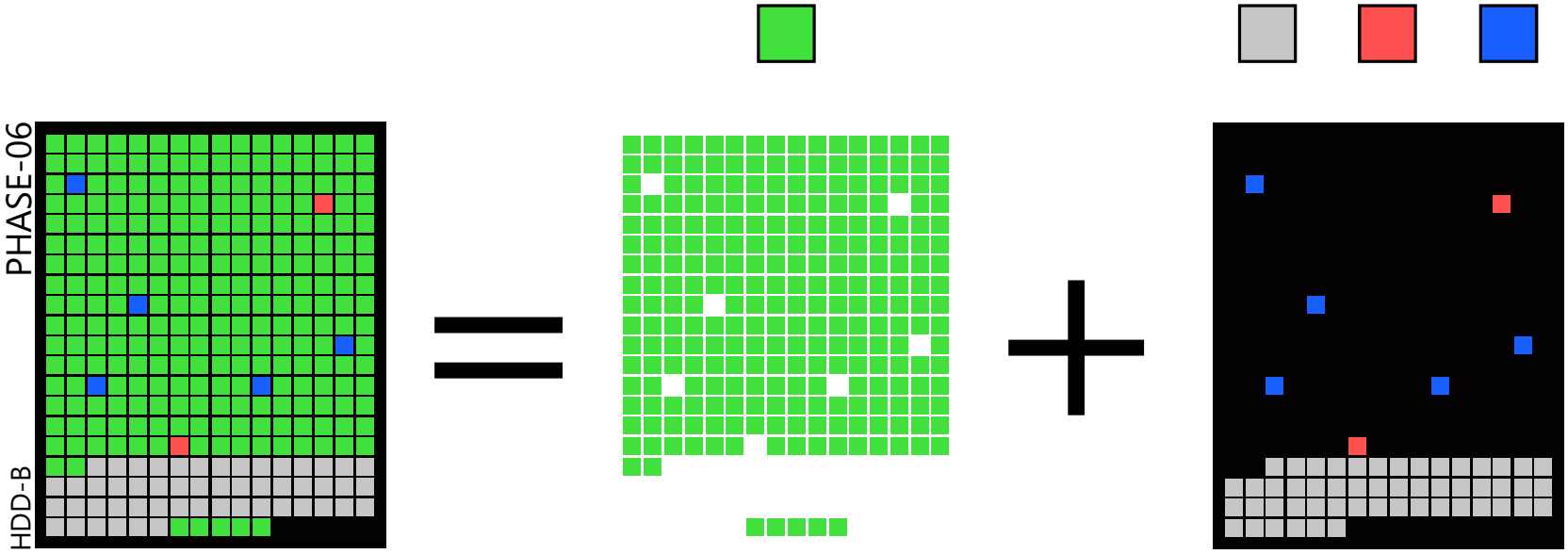
代替処理後の不良セクタ

HDD - 保全解析の対象と非対象領域



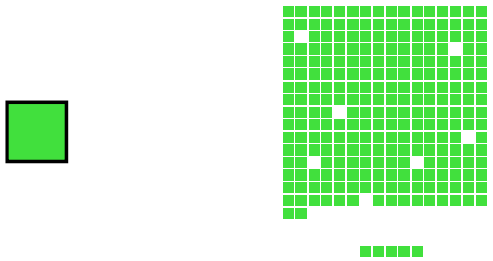
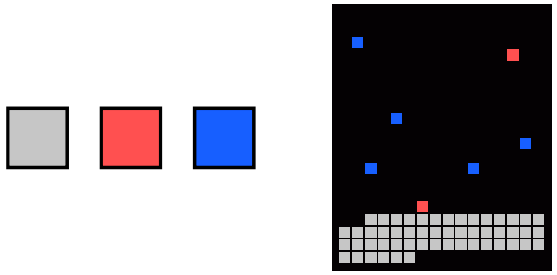
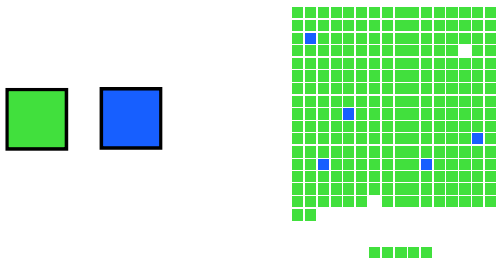
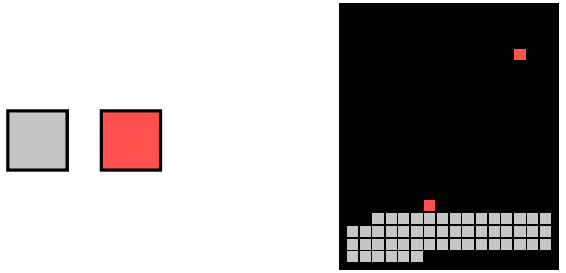
- LBAが割り当てられていないセクタ
- LBAが割り当てられているセクタ
- 製造段階でLBAの割り当てが除外されたセクタ
- 代替処理後の不良セクタ

HDD - データ消去の対象と非対象領域

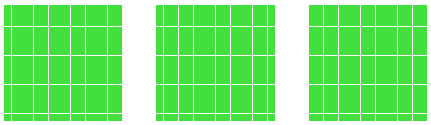


- LBAが割り当てられていないセクタ
- LBAが割り当てられているセクタ
- 製造段階でLBAの割り当てが除外されたセクタ
- 代替処理後の不良セクタ

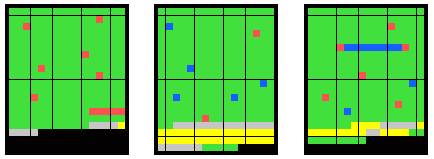
HDD - データ消去の対象と非対象領域

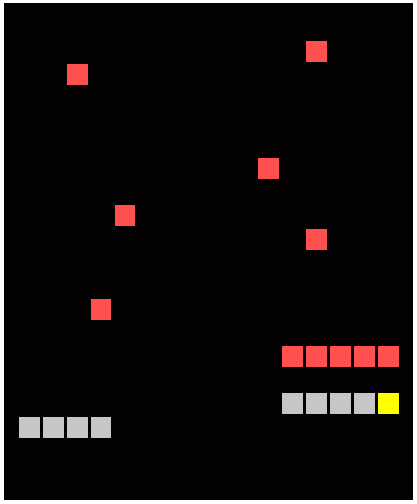
	消去可	消去不可
データ消去ソフト・ツール Secure Erase DoD方式（米国国防総省） グートマン方式（35回） ※物理破壊は除く		
Enhanced Secure Erase （NIST）		

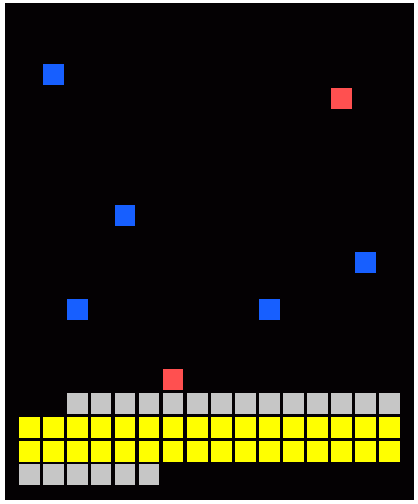
- LBAが割り当てられていないセクタ
- LBAが割り当てられているセクタ
- 製造段階でLBAの割り当てが除外されたセクタ
- 代替処理後の不良セクタ

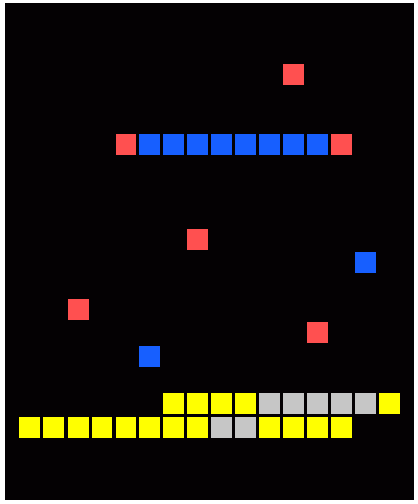


データ消去









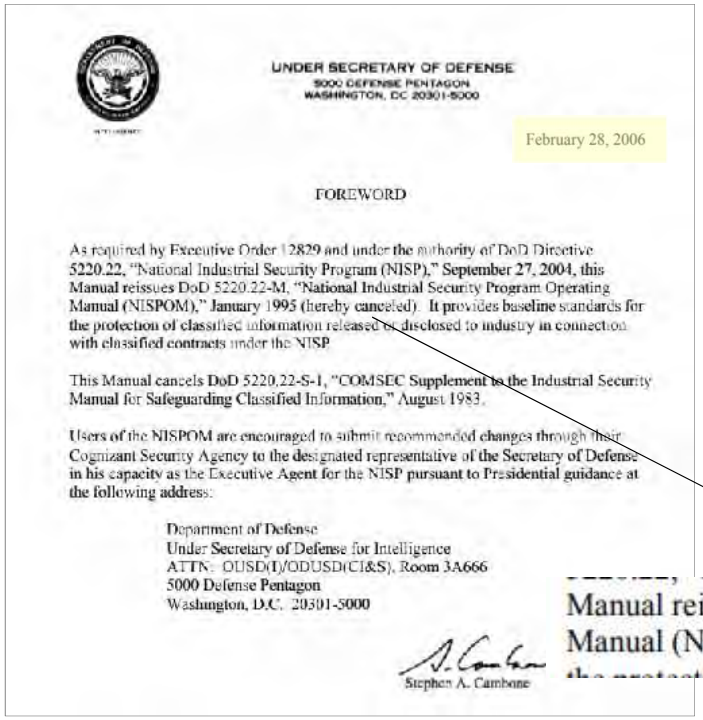
HDDを**完全消去**できるソフトウェアは**無い**

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(CI&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

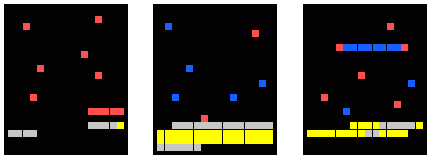
DoD（米国国防総省）準拠方式

DoD5220.22-M

2006年に破棄済み

検討すべき課題

デジタル・フォレンジック

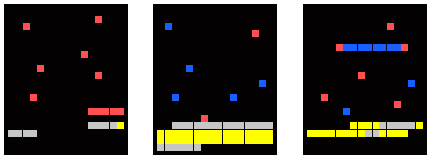


捜査機関

裁判所

検討すべき課題

デジタル・フォレンジック



捜査機関　　裁判所