

サイバー部門だけでなく全捜査員必読!
初動対応や捜索時の留意点が満載!

デジタル鑑識の基礎(上) 第2版

「証拠ファイルが削除されている!」~残存データの可視化技術

一般財団法人 保安通信協会 編著

- A4判 ● 80頁・2色刷
- 定価1,100円(本体1,000円+税10%)
- ISBN978-4-8090-1435-2 C3055 ¥1000E

本書の特色

最新のデジタル鑑識情勢を踏まえ、
内容をアップデート!
法執行機関職員の業務に沿った内容を追加!

- ◆ デジタル鑑識の基礎知識を、図表・写真・イラストを豊富に用い、初心者にも分かりやすく解説!
- ◆ 技術的な解説にとどまらず、実戦的なデジタル鑑識のノウハウとして、現場での具体的な初動対応や捜索時の留意点にも踏み込んで解説!
- ◆ 新たにファイルシステムについて解説し、巻末では、最新のデジタル鑑識用ツール、サービス等を紹介。
- ◆ 上・中・下巻、どの巻からも気軽に読み進められる、使いやすい構成。

詳細は
こちら!



内容見本

3.6.1 MBRの構造

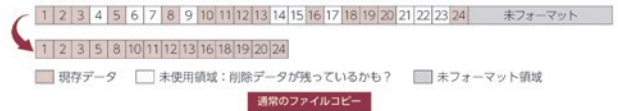
- MBRのパーティションテーブルには以下の情報が記録されています。
- ・ブートフラグ (当該パーティションの起動可否を記録)
 - ・パーティション開始位置 (CHS形式)
 - ・パーティションタイプ (パーティションのフォーマット形式)
 - ・パーティション終了位置
 - ・パーティション開始位置 (LBA形式)
 - ・パーティション総セクタ数 (総セクタ数をLBA形式で記録)

オフセット	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	
0x0000	33 C0 8E D0 BC 00 7C 8E	C0 8E D8 BE 00 7C BF 00	ブートストラップローダ (446Byte)
0x0010	06 B9 00 02 FC F3 A4 50	68 1C 06 CB FB B9 04 00	
0x0020	BD BE 07 80 7E 00 00 7C	0B 0F 85 0E 01 83 C5 10	
0x0030	E2 F1 CD 18 88 56 00 55	C6 46 11 05 C6 46 10 00	
0x0180	20 6C 6F 61 64 69 6E 67	20 6F 70 65 72 61 74 69	パーティションテーブル
0x0190	6E 67 20 73 79 73 74 65	60 00 4D 69 73 73 69 6E	
0x01A0	67 20 6F 70 65 72 61 74	69 6E 67 20 73 79 73 74	
0x01B0	65 60 00 00 00 63 78 9A	19 91 9C 1A 00 00 00 20	
0x01C0	21 00 27 FE FF FF 00 08	00 00 00 18 D9 02 80 FE	エン트리 4 (16Byte)
0x01D0	FF FF 07 FE FF FF 00 20	D9 02 00 F0 0A 00 00 FE	ブートシグネチャ (2Byte)
0x01E0	FF FF 07 FE FF FF 00 10	E4 02 00 A0 B9 37 00 FE	
0x01F0	FF FF 0F FE FF FF 00 80	90 3A 00 88 00 01 55 AA	

図表を用いて
分かりやすく
解説!

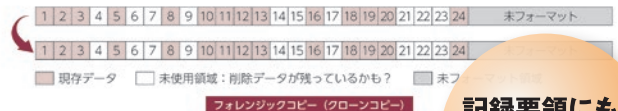
1.6.3.1 ◆複製作成における技術的要綱：通常のコピーとフォレンジックコピーの違い

では、**【完全な複製】**とはどのようなことを指すのでしょうか?
例えば Windows 起動後に、Cドライブ配下の全データを選択し、外付けハードディスク等に**コピー&ペースト** (貼り付け) をしたと仮定します。
この操作は通常の**ファイルコピー** (【論理コピー】と呼ばれることもあります) 操作になりますが、このときにコピーされるデータは**【ユーザからアクセス可能な現存データのみ】**であり、削除されたデータが残っている可能性のある未使用領域や未割り当て領域はコピーされないため、完全な複製とはいえません。



上図は通常の**ファイルコピー**の概念を簡単に表したものです。ファイルコピーでは、現存するデータ部分のみがコピーされるだけであるため、コピーの対象外となる未使用領域や未フォーマット領域に対する調査はできません。

通常の**ファイルコピー**に対し、デジタル・フォレンジックにおける**【完全な複製】**とは、ハードディスク、SSD、USBメモリ等の記録媒体上に「0」若しくは「1」が割り振られたビット単位の情報を、記録媒体上の物理的な格納場所も維持したまま別の記録媒体にコピーすることをいい、この手法は**フォレンジックコピー**とも呼ばれています。



記録要領にも
触れながら
実践的に解説!

上の図には MBR の構造例を示しています。パーティションテーブルエントリが 4 つ記録されていることから、この MBR を持つハードディスクには、4 つのパーティションが存在するものと見なされます。

本書の構成

1 デジタル鑑識の概要

- 1.1 「フォレンジック」とは?
- 1.2 デジタル・フォレンジックが必要な理由
- 1.3 デジタル・フォレンジックの目的
- 1.4 デジタル・フォレンジックの用途
- 1.5 デジタル・フォレンジックの種類 (分野)
- 1.6 デジタル・フォレンジックの作業フロー

2 デジタルデータの基礎

- 2.1 デジタルデータの特徴
- 2.2 デジタルデータとは何なのか?
- 2.3 数値表現方法の種類と変換
- 2.4 デジタルデータの単位
- 2.5 ファイル
- 2.6 ファイルシステム
- 2.7 ファイルの識別

3 コンピュータの基礎

- 3.1 コンピュータの種類
- 3.2 コンピュータの5大装置
- 3.3 コンピュータの内部構造
- 3.4 BIOS (バイオス)
- 3.5 ブートプロセス
- 3.6 MBRの情報
- 3.7 ハードディスクにおけるデータ管理の概念

4 デジタル鑑識の実務

- 4.1 「デジタル鑑識」の対象
- 4.2 デジタル・フォレンジックのツール
- 4.3 フォレンジック環境の構築
- 4.4 必要となるフォレンジック作業の判断

索引 (50音順)

巻末参考

デジタル・フォレンジック用ツール、サービス等

あわせて読みたい!『デジタル鑑識の基礎』シリーズ。好評発売中!

デジタル鑑識の基礎(中)

—インシデントレスポンスと初動対応—

一般財団法人 保安通信協会 編著

● A4判 ● 64頁・2色刷 ● 定価917円(本体834円+税10%)
ISBN978-4-8090-1380-5 C3055 ¥834E

本書の特色

- ◆ 難解な情報セキュリティ事案への対応を、コンパクトに解説した、画期的入門書。
- ◆ インシデント(コンピュータやネットワークのセキュリティを脅かす事象)に備える組織体制の構築や、デジタル・フォレンジックとの関係をも解説した実践的な内容。

デジタル鑑識の基礎(下)

—証拠保全—

一般財団法人 保安通信協会 編著

● A4判 ● 64頁・2色刷 ● 定価917円(本体834円+税10%)
ISBN978-4-8090-1398-0 C3055 ¥834E

本書の特色

- ◆ 「デジタルデータの証拠保全」に必要な基礎知識を、現場での具体的な初動対応や捜索・押収時の留意点にも踏み込んで解説!
- ◆ 実践的な証拠保全のノウハウを、図表、チャートを交えて解説。

申込書

デジタル鑑識の基礎(上) 第2版 定価1,100円(本体1,000円+税10%) (コード12841)	申込	部	送料は実費 税込購入金額3,000円 以上はサービス
デジタル鑑識の基礎(中) 定価917円(本体834円+税10%) (コード13106)	申込	部	
デジタル鑑識の基礎(下) 定価917円(本体834円+税10%) (コード13288)	申込	部	

貴社の個人情報に関する下記取扱いに同意し、上記のとおり申し込みます。

(フリガナ)

お取扱者(自署) (TEL - -)

お届け先 〒

団体名 部署名 公用 私用

個人情報の取扱いについて 東京法令出版株式会社 個人情報保護管理者 専務取締役

- ★お客様の個人情報は、契約の履行及び関連製品の案内に利用します。
- ★本人の同意がある場合又は法令に基づく場合を除き、第三者に提供しません。
- ★利用目的の達成に必要な範囲内で取扱いの一部を委託することがあります。
- ★本人からの個人情報の利用目的の通知・開示・内容の訂正・追加又は削除・利用の停止・消去の求めに応じます。
- ★個人情報に関するご照会・お問い合わせ等は、弊社窓口(TEL026-224-5441、privacy@tokyo-horei.co.jp)までご連絡ください。
- ★お申込みには個人情報の提供が必要です。提供いただけない場合は、お申込みをお受けできないことがあります。

東京法令出版公式 Twitter アカウント

@tokyo_horei



この申込書は、このままFAXで下記宛にお送りください。

■申込先 東京法令出版 受注センター
〒381-0022 長野市大島3111

FAX 0120-338-923

TEL 0120-338-272 (携帯電話からもお申込みできます。)

会社使用欄	団体コード		<input type="checkbox"/> 納品済	入力印	
	得意先コード		<input type="checkbox"/> 請求済		
	在庫	ラベル	〒	チェック	