

「デジタル・フォレンジック」の重要テーマを
最もコンパクトに解説した入門シリーズ、

3部作完結!

一般財団法人 保安通信協会 編著

シリーズ
の特色

- ◆ 法執行機関職員、法曹の捜査・公判対応や、企業の不祥事案調査に必須の基礎知識を凝縮!
- ◆ 図表・写真を豊富に用い、初心者にも分かりやすく解説!
- ◆ 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!

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



東京法令出版

新刊

デジタル鑑識の基礎(下) — 証拠保全 —

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

下巻の特色

- ◆ 「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!
- ◆ 技術的な解説にとどまらず、実戦的な証拠保全のノウハウを、図表、チャートを交えて解説!

好評
既刊

デジタル鑑識の基礎(上)

● A4判 ● 48頁・2色刷 ● 定価(本体556円+税)
ISBN978-4-8090-1358-4 C3055 ¥556E

(主な構成)

- 1 デジタル鑑識の概要
1.1 デジタル・フォレンジックとは
- 2 デジタルデータの基礎
2.1 デジタルデータの特徴
- 3 コンピュータの基礎
3.1 コンピュータの種類



好評
既刊

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 —

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

(主な構成)

- 1 インシデントレスポンスの概要
- 2 デジタル・フォレンジック作業における初動対応
2.3 初動対応者となった場合に備え
2.4 調査対象選定について
2.5 初動対応(現場対応)における問題点



詳しくは裏面へ

東京法令出版

詳しい内容は、こちらまで!

東京法令

検索

<https://www.tokyo-horei.co.jp/>



フォレンジック基礎講座のエッセンスを凝縮!

(下) 目次

1 デジタル・フォレンジックの概要

1.1 デジタル・フォレンジックの目的 / 1.2 デジタル・フォレンジックの分類 / 1.3 デジタル・フォレンジックの作業フロー

2 証拠としてのデジタルデータ

2.1 そもそも証拠とは / 2.2 「写し」による提出形態 / 2.3 証拠として提出されたデジタルデータの原本性 / 2.4 証明力(証拠力)と証拠能力

3 証拠保全概論

3.1 証拠保全の目的 / 3.2 証拠保全作業従事者に求められるスキル / 3.3 証拠保全で用いられるデータコピー方法 / 3.4 デジタルデータの同一性検証

4 証拠保全作業の流れ

4.1 ①: 事前準備 / 4.1.1 事前準備: コピー先ハードディスクのデータ消去 / 4.1.2 事前準備: コピーツール付属品の動作確認 / 4.1.3 事前準備: 工具備品類 / 4.1.4 事前準備: 記録用紙 / 4.1.5 事前準備: 情報収集 / 4.2 ②: 物品の押収 / 回収 / 4.3 ③: ハードディスク取り外し / 4.4 ④:

データコピー / 4.5 ⑤: ハードディスク取り付け / 4.6 ⑥: 物品の返却 / 4.7 ⑦: コピー先ハードディスクの取り扱いについて

5 証拠保全ツールに求められる機能要件

6 証拠保全方法の選択

6.1 ハードディスクの取り外しが可能なパソコンへの対応 / 6.2 ハードディスクの取り外しが困難なパソコンへの対応 / 6.3 ソフトウェアによる証拠保全 / データコピー / 6.4 ファイルレベルでのデータ取得について

7 揮発性情報の取得について

8 モバイル端末のデータ取得について

8.1 初動対応での注意点 / 8.2 データ取得方法 / 8.3 データの格納先 / 8.4 モバイル端末データのハッシュ値

9 セキュリティ設定への対応

9.1 BIOSパスワード (Power-on Password) / 9.2 ハードディスクパスワード / 9.3 ハードディスク (デバイス) 暗号化 / 9.4 フォルダ/ファイル暗号化

2.4 証明力(証拠力)と証拠能力

2.1 項では、「証拠とは事実認定の根拠となる資料のこと」として「証明力(証拠力)と証拠能力」という、2つの観点から考慮する必要がある証拠に対して「証明力(証拠力)を判断する」としています。

証明力(証拠力)	証明力とは、「 事実認定に寄与し得るか否かの美 」(証明力)は、民事訴訟法第247条(注)及び刑事訴訟法第306条に「 自由心 」とすることが定められています。
証拠能力	証拠能力とは、「 事実認定の証拠として適用可能な資格 」といえ、民事訴訟では、原則、証拠能力を否定されることはないといわれていますが、刑事訴訟においては、証拠能力が厳格に定められており、「 自然的関連性/法律的関連性 」があり、かつ、「 証拠禁止にあたらないこと 」が求められます。なお、「 証拠禁止にあたらないこと 」の例としては、証拠物品の押収/回収時において、押収/回収方法に違法性があつた場合、その証拠能力は否定されることとなります。

このような証明力(証拠力)と証拠能力の関連性を考えた場合、フォレンジック調査結果として提出された紙媒体やデジタルデータに対して、証明力が認められ、事実認定の資料として適用されるためには、**証拠物品の押収/回収において違法性がないこと**は大前提であり、かつ、**図3**で示すように、提出記録媒体内のデジタルデータから、調査対象として押収/回収されたパソコンやUSBメモリ等に格納(保存)されている「**原本**」が、提出データの出力として**層層可能な途中経過と状況を示すことが可能な情報(作業証拠)**が残され、それら資料を**法的/合理的な事実認定が可能であること**が必要であるといえるのではないのでしょうか。

またこのことは、2.3項で記した提出したデータの真正性や信頼性、真実性の証明にもつながるのではないのでしょうか。



内容見本

8 モバイル端末のデータ取得について

これまで本書では、ハードディスク内データやUSBメモリ等の外部記録媒体の証拠保全について解説してきましたが、昨今の調査現場で急増している事例は、いさよほど出現頻度の低い記録媒体が、スマートフォンに代表される**モバイル端末**です。モバイル端末のデータ取得は、ハードディスクやUSBメモリ等の外部記録媒体の証拠保全と比較した場合の取得方法のほとんどが、**モバイル端末専用のソフトウェア**によるものとなります。しかし、モバイル端末からのデータ取得方法が統一/確立されていない現状に加え、各メーカーやキャリアメーカーの開発速度も速く、同一モデルでもキャリアが異なることや、OSバージョンによっては同じ取得方法が適用できない場合もあることに加え、ソフトウェアごとに対応種や取得可能なデータの異なるため、何がどれくらい取得可能なかも明確ではなく、後手に回った対応となっていることは否めません。このような事情下にあるモバイル端末ですが、証拠保全対象物として考えた場合、どのような点に注意する必要があるか、又は、何が問題点なのかを考察していきましょう。

8.1 初動対応での注意点

モバイル端末であっても、電子記録媒体としての取扱いは、パソコンやUSBメモリ等の記録媒体類と変わりませんが、モバイル端末が持つ特徴から、物品の押収/回収後は、以下に挙げる行動を取る必要があります。

- ☑ ネットワークからの情報
 - ☑ 既 (Airplane) モードをオンにする。
 - ☑ Wi-Fi、Bluetooth 機能をオフにする。
 - ☑ 電源遮断シールドボックスや、電源遮断袋(モバイル端末を格納する)。
- ☑ 比較的単純な4桁のセキュリティコードの場合、使用するモバイル端末専用ソフトウェアによっては、クラックが可能である場合がある。
- ☑ 所有客又はシステム部門等の端末管理者から、スライドボタン(リターンコード)を入力する。
- ☑ Android 端末の場合、USB Debugging をオンにする。
 - ※ オフのままではデータ取得が困難
 - ☑ USB Debugging は設定画面からオンにすることが多いため、実質的に端末アンロックが必要となる(セキュリティコードが必要となる)。

取扱いが増えているモバイル端末からのデータ取得についても解説!

4 証拠保全作業の流れ

4.1.4項で記した**撮影用タグ**を用いて、個体識別のための**写真撮影**を行うことが非常に重要となります。作業担当者自身が、**詳細な作業記録**を残しておくことも重要になります。加えて、物品の押収/回収においては、必要に応じ、対象物品に接続されている電源ケーブルやマウス/キーボード等の、**周辺機器や付属品も押収/回収**する必要があります。また、それら周辺機器も含めた物品の押収/回収の前に、**図17**のように電源ケーブル等の各ケーブルが接続されている状態を写真撮影を行い、**機器類の位置関係等の状況**を記録しておくことが必要です。電源ケーブルの接続口が異なる場合、パソコンから認識できないため、**物品返却時に押収/回収時の状態に戻す**ために、各ケーブルには付箋紙やラベルシールを貼付し、接続箇所が明確に判断可能なように構成する必要があります。



図17 接続ケーブル撮影の例

また、証拠物品としては、種類や借取を所有者と調査員(受調者)との間で署名確認を行いその物品は**図18**のような**証拠品台帳(管理表)**を作成し一元管理をするなど、物品の管理についても、効率的な証拠品管理につながります。

品番	名称	数量	備考
PC_001	デスクトップPC	1台	証拠品
PC_002	モニター	1台	証拠品
PC_003	キーボード	1台	証拠品
PC_004	マウス	1台	証拠品
PC_005	電源ケーブル	1本	証拠品
PC_006	USBケーブル	1本	証拠品
PC_007	周辺機器	1台	証拠品

図18 証拠品管理表の例

なお、パソコン筐体を分解する可能性がある場合、所有者には物品の押収/回収時に**分解の可能性、並びに**分解を行ったことによる**メーカー保証外となる可能性**を説明した上でその承諾を得て、承諾されたことを記録簿に明記しておくことが良いでしょう。

申込書

新刊 デジタル鑑識の基礎(下) - 証拠保全 - 定価(本体834円+税) [コード13288]	申込部	送料は実費。ただし、税込購入金額3,000円以上はサービス
既刊 デジタル鑑識の基礎(上) 定価(本体556円+税) [コード12841]	申込部	
既刊 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 - 定価(本体834円+税) [コード13106]	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。 年 月 日

お取扱者(自署) (TEL - -)

〒

お届け先住所

団体名 部署名

公用 私有

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 株式会社** 受注センター
〒381-0022 長野市大豆島3111

FAX 0120-338-923
TEL 0120-338-272 (携帯電話からも申込みできます。)

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(TEL.026-224-5441, privacy@tokyo-horei.co.jp)までご連絡ください。
★個人情報の提供は任意ですが、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。

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	チャック
	在庫	<input type="checkbox"/> 領収済	
	ラベル	〒	チャック