デジタル・フォレンジック・プロフェッショナル認定
（Certified Digital Forensic Profesional）

デジタル・フォレンジック基礎資格（CDFP－B）認定試験シラバス第1版

2020年8月14日

特定非営利活動法人デジタル・フォレンジック研究会

デジタル・フォレンジック資格認定WG

1 デジタル・フォレンジックの基礎知識 （参考書(注1) 第1章）

(注1)「参考書」は、「安富 潔・上原 哲太郎 編著『基礎から学ぶデジタル・フォレンジック』日科技連出版社、2019年」を示す。

(注2)「NIST SP800-86」の例を示す。

大項目	中項目	小項目	備考
状況によってデジタル・フォレンジックの定義が使い分けられていることを理解する デジタル鑑識とデジタル・フォレンジックの用法の違いについて理解する	司法機関が犯罪立証に用いる定義		
	一般にインシデントレスポンスや法的紛争・訴訟に対して用いる定義		
	デジタル鑑識の用法とデジタル・フォレンジックとの違い		
デジタル・フォレンジックの分類軸を理解する	デジタル・フォレンジックを利用する主体の分類		
	訴訟の対象となる行為の分類		
	訴訟の種類による分類	民事訴訟	
		刑事訴訟	
	訴訟との関連における分類	訴訟を提起する側	
		訴訟提起を受ける側	
	電磁的記録を保持する機器による分類		
	電磁的記録を保管する媒体による分類		
	証拠となる電磁的記録の種類による分類	ログ	
		痕跡	
	証拠性の保持に関連するアプリケーションソフトによる分類		
	情報システムの運用形態による分類	オンプレミス	
		クラウド	

大項目	中項目	小項目	備考
デジタル・フォレンンジックに関連する用語 について理解する	対象機器による命名	コンピュータ・フォレンジック	
		ネットワーク・フォレンジック	
		モバイル・フォレンジック	
		メモリ・フォレンジック	
	運用形態による命名	クラウド・フォレンジック	
	フォレンンジックのやり方による命名	ライブ・フォレンジック	
		ファスト・フォレンジック	
デジタル・フォレンジックの手順について理解する	収集・検査・分析・報告(注2)		
デジタル・フォレンンジックにおいて必要となる技術 について理解する	対象となる電磁的記録を選択する技術		
	保全した電磁的記録の消去や改ざんを防止する技術		
	保全対象となる媒体の完全消去技術		
	保全の際の物理コピー技術		
	電磁的記録の検索技術		
	削除ファイルや破損媒体の復元技術		
	暗号化されたデータの復号技術		
	大量データから有用なデータを抽出する技術		
	調査不正がないことの心証形成技術		
デジタル・フォレンンジックの作業における注意事項 について理解する	プライバシーとの関連		
	早急な対応との関連	証拠性の確保	
コンピュータや補助記憶装置について理解する	コンピュータの基本構成		
	補助記憶装置の種類	磁気媒体	
		光学媒体	
		半導体による媒体	

大項目	中項目	小項目	備考
証拠保全対象の多様化による問題について理解する	SSDの問題		
	ハードディスクの大容量化問題		
	その他の多様化問題		
OSやファイルの基本について理解する	データ表現	数値表現	
		文字コード	
		音声や画像	
		Webページ・メール・文書・スプレッドシート	
		圧縮データ	
	ファイルシステムの基本的機能		
	証拠保全の対象となるファイル		
デジタル・フォレンンジックの一般的手順について理解する	対象機器		
	事前に準備するもの		
	一般的な手順		

2 デジタル・フォレンジック実務全般の知識（参考書 第2章）

大項目	中項目	小項目	備考
データ収集（証拠保全）作業に関する基礎知識	データ収集の実務全般における留意点について理解する	揮発性が高く書き換わりやすいデータの取り扱い	
		フォレンジックコピーの必要性	
		ハッシュ値による同一性の証明	
	データ収集前における起動中端末の取り扱いについて理解する		
	データ収集前における証拠端末のセキュリティ解除の影響について理解する	BIOSパスワード	
		HDDパスワード	
		HDD暗号化	
	クラウドやファイルサーバからのデータ収集時の留意点について理解する	フォルダやファイルレベルでのデータ収集	
データ復元作業に関する基礎知識	ファイル保存の仕組みについて理解する	ファイルシステムによる管理とデータ本体の断片化	
	ファイル削除とデータ復元の仕組みについて理解する	ファイルシステムの管理情報からのデータ復元	
	高度な復元（データカービング）の仕組みについて理解する	ファイルシグネチャを活用したデータ本体からのデータ復元	
	コンピュータ上の動作によるデータ復元への影響について理解する	論理フォーマット（クイックフォーマット、標準フォーマット）	
		完全消去（上書き消去）アプリケーション	
		デフラグメンテーション	
	磁気ディスク（HDD）から半導体メモリ（SSD）への変更に伴う影響について理解する		

大項目	中項目	小項目	備考
データ分析作業に関する基礎知識	データ分析の主要な2つのアプローチについて理解する	タイムライン分析	
		ファイル内容解析	
	時間とイベントが紐づいたタイムライン分析のアプローチについて理解する	タイムスタンプ	
		レジストリファイル	
		イベントログ	
		プリフェッチファイル	
		ショートカットファイル	
	オフィスファイルやEメールなどファイル内容分析のアプローチについて理解する	文字コード	
		キーワード検索（ブーリアン/正規表現/近傍）	
	人工知能の活用について理解する	教師データの学習と調査対象データのスコアリング	
報告書作成時における留意点	コンピュータ・フォレンジック調査報告書に必要となる要件について理解する	公平であること	
		客観的であること	
		真正であること	
		理解可能であること	
		再現性があること	
	コンピュータ・フォレンジック調査報告書に記載すべき事項について理解する		
コンピュータ・フォレンジック調査のポイント	データ収集時におけるHDDボリューム全体暗号化の影響について理解する	HDD暗号化の種類（BitLocker/FileVault2/PGP/SafeBoot）	
		HDD暗号化設定の確認方法	
	HDDボリューム全体暗号化されたPCのデータ収集時の注意点を理解する	ネットワークからの遮断	
		ログオンIDとパスワードの入手	

大項目	中項目	小項目	備考
コンピュータ・フォレンジック調査のポイント	目的を限定したファイルレベルでのデータ収集を理解する		
	コンピュータ・フォレンジックにおいて必ず調査すべきポイントを理解する	Windows PCにおけるポイント	
		Mac PCにおけるポイント	
スマートフォンを対象にしたデジタル・フォレンジック(モバイル・フォレンジック)調査のポイント	モバイル・フォレンジックの初動対応時の留意点について理解する	通信の遮断	
		電源はOFFにしない	
	モバイル・フォレンジックのデータ収集(証拠保全)手法について理解する	スマートフォンのバックアップ機能を利用した手法	
		スマートフォンのアプリケーションを利用した手法	
		カスタムROMブートによる手法	
		JTAGによる手法	
		チップオフによる手法	
	スマートフォンのroot化やJailbreakの影響について理解する		
	モバイル・フォレンジックのデータ収集時における原本との同一性確認の困難性について理解する		
	SQLite3データベースの解析について理解する		
	クラウド上に残るモバイル端末のバックアップデータについて理解する		
ネットワーク・フォレンジック調査のポイント	コンピュータ・フォレンジックとネットワーク・フォレンジックとの違いについて理解する	トラフィックデータに関わるログ取得の必要性	
	ネットワーク・フォレンジックの主な目的について理解する	状況認識のための情報収集	
		事実認定に備えた証拠の取得・保全	
		セキュリティ対策のための侵入検知	

大項目	中項目	小項目	備考
ネットワーク・フォレンジック調査のポイント	ネットワーク・フォレンジックの対象 について理解する	イーサネット	
		TCP/IPプロトコル	
		サーバソフトウェア	
	ネットワーク・フォレンジックの基本的な流れ について理解する	インシデント検知	
		コンピュータネットワーク環境の保全	
		証跡・ログの収集	
		検索・抽出	
		分析	
		報告資料作成	
	ネットワーク・フォレンジックにおける課題 について理解する	暗号化	
		スプーフィング（なりすまし）	
		プロキシ（中継）	
ファスト・フォレンジック調査のポイント	ファスト・フォレンジックとはどのような 調査か理解する	早急な実態解明と原因追及	
		侵入経路や不正挙動の把握 に特化した必要最低限の データ抽出と解析	
	ファスト・フォレンジックが注目される 背景・理由について理解する	コンピュータ内のデータ容量の増加	
		ネットワークを介した他のコンピュータ への感染拡大（ラテラルムーブメント）	
		ファイルレス攻撃の増加	
	ファスト・フォレンジックの具体的な作業 について理解する	揮発性情報のデータ収集と解析	

3 調査・捜査とデジタル・フォレンジックの実務（参考書 第3章）

大項目	中項目	小項目	備考
不正調査に使われる デジタル・フォレンジックを理解する	不正や不祥事の態様による分類		
	不正調査の流れ	初動調査	
		実態調査	
		是正措置策定	
		ステークホルダー対応と公表	
情報漏洩事案に使われる デジタル・フォレンジックを理解する	情報漏洩の種類		
	情報漏洩に関する法制度		
	情報漏洩に関する課題		
企業における情報管理に使われる デジタル・フォレンジックを理解する	クラウドと情報管理		
	企業の情報管理と デジタル・フォレンジックの関係		
	情報管理ツールや端末管理ソフトと デジタル・フォレンジックの関係	端末セキュリティ管理ツール	
		モバイル端末管理ツール	
		クラウドセキュリティ管理ツール	
第三者委員会に使われる デジタル・フォレンジックを理解する	調査委員会の種類		
	第三者委員会における調査の進め方		
	第三者委員会における調査の課題		
犯罪捜査に使われる デジタル・フォレンジックを理解する	犯罪捜査におけるデジタル・フォレンジック の各手続	記録命令付差押	
		電磁的記録に係る記録媒体の差押	
		リモートアクセスによる複写の処分	
	アンチフォレンジック		

4　訴訟とデジタル・フォレンジックの実務　その1（参考書　第4章　4.1節、4.2節）

大項目	中項目	小項目	備考
刑事裁判はどのように進むのかを理解する	犯罪の発生から捜査, 起訴, 公判手続, 判決という手続の流れを知る		
	公判前整理手続という手続の目的と手続を知る		
	公判という手続がどのように進行するかを知る	冒頭手続	
		証拠調べ（冒頭陳述, 証拠調べ, 弁論）	
		証拠の種類（物証, 人証, 書証）	
	証拠調べの方法を知る		
	デジタル証拠の取調べはどのように 実施されるかを知る		
	捜査機関の作成した書面はどのように 証拠調べが実施されるかを知る		
刑事訴訟での証拠に関するルールを理解する	事実の認定は証拠によらなければならない という原則を理解する		
	証拠とは法律上どのような意味かを知る		
	証拠能力と証明力の意味を知る	証拠能力	
		証明力	
	刑事訴訟で証拠はどのような要件を満たせば 証拠として用いられるかを知る		
	証拠法則に関して民事訴訟と刑事訴訟とでは 異なることを理解する		
	刑事訴訟における証拠に関する法則を理解する	違法収集証拠	
	自白法則とはどのような法則かを理解する	自白	
		任意性	

大項目	中項目	小項目	備考
刑事訴訟での証拠に関するルールを理解する	伝聞法則とはどのような法則かを理解する	伝聞証拠	
		伝聞法則とその例外	
	捜査機関の作成した書面が証拠となるには どのような要件が必要かを知る		
	デジタル・フォレンジックを用いて解析された 証拠が証拠となる場合を知る		
裁判員裁判におけるデジタル証拠と デジタル・フォレンジックの利用を理解する	裁判員の参加する刑事裁判(裁判員裁判)が どのような裁判かを知る		
	裁判員裁判でデジタル・フォレンジックを用いて 解析された証拠がどのような場合に用いられるか 事例を知る		
	デジタル・フォレンジックを用いて解析した結果を 証拠として犯罪事実を認定するにはどのような ことに留意しておくかを知る		

5 訴訟とデジタル・フォレンジックの実務 その2

（1） 国内民事訴訟法の基礎知識（参考書 第4章 4.3節～4.5節）

大項目	中項目	小項目	備考
デジタル・フォレンジックにいう一般的な証拠保全と民事訴訟法における証拠保全との違いを理解する	裁判官が実際に現場に赴いて検証を実施する民事訴訟法の証拠保全		
	正式裁判（本案）を提起する前に実施する証拠保全		
	民事訴訟法の証拠保全により行う証拠調べの方法（検証・書証・人証・その他）		
	民事訴訟法の証拠保全の強制力の有無、拒否した場合の効果		
民事訴訟法と電子署名・認証法における成立の真正を理解する	形式的証拠力と実質的証拠力との違い		
	二段の推定と押印（実印と認印）		
	電子署名・認証法における真正な成立の推定		
国内の民事訴訟手続におけるIT化の動向と課題を理解する	3つのe（e-提出、e-事件管理、e-法廷）の各内容		
	本人訴訟（代理人をつけずに遂行する訴訟）におけるIT化の課題と特徴		
	民事訴訟手続のIT化における情報セキュリティ対策の課題と特徴		
	民事訴訟におけるC（機密性）・I（完全性）・A（可用性）の具体例		
	民事訴訟手続のIT化の法改正に向けた動き		

（2）アメリカ民事訴訟法の基礎知識（参考書　第4章　4.6節）

大項目	中項目	小項目	備考
eディスカバリの基本的な仕組みを理解する	ESI（電子的に保存された情報）		
	eディスカバリにおける開示の対象・要件	関連性	
		弁護士と依頼者との間の秘匿特権（法律上の助言を求めるに際し、弁護士と依頼者との間で交わされたコミュニケーションについては開示を拒否できるという特権）	
		ワークプロダクト（訴訟の準備のために弁護士が活動した成果として作成した文書等は、ディスカバリの対象から除外できる制度）	
		費用対効果、その他諸事情の考慮	
	メタデータの開示		
	TAR（テクノロジー支援レヴュー：少数のドキュメントセットに関する対象分野の専門家の人間の判断を利用し、その判断から残りの収集ドキュメントの関連性等について、コンピュータ・システムを使って推定しドキュメントの優先順位付けやコーディングを行う処理）		
アメリカ民事訴訟の基本を理解する	リティゲーション・ホールド（訴訟提起が合理的に予想される時点において当事者に課される証拠の保存義務、あるいは、同時点において訴訟に関連するESIや文書を削除・破棄等しないよう関係者に送る通知）		
	サピーナ（特定の日時に特定の場所に出頭すべきことを命じる裁判所の罰則付きの命令）		

大項目	中項目	小項目	備考
アメリカ民事訴訟の基本を理解する	デポジション（法廷以外の場所において、宣誓させる権限のある者の前で、尋問形式でなされる供述録取の手続）		
	サマリー・ジャッジメント（重要な事実について真の争点がなく、法律問題だけで判決の言い渡しができる場合に、トライアルを経ることなく当事者の申立てによって裁判所が下す判決）		
	トライアル（原告と被告双方が裁判所の面前で正式に行う事実審理）		
	陪審員裁判と裁判官裁判		