デジタル・フォレンジック実務者資格（CDFP－P）シラバス案　＜技術系＞

大項目	中項目	小項目	CDFP-B(注1)	CDFP-P (注2)
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	電子機器/精密機器の取り扱い	○	
		対象媒体の情報収集	○	
		BIOS/UEFI	○	○
		RAID構成のコンピュータの取り扱い		○
		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	○	
		書込防止措置（媒体の書込防止スイッチ、ライトブロッカー）		○
		データ収集の手法	○	○
	データ収集前における起動中端末の取り扱い		○	
	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	BIOSパスワード	○	
		HDDパスワード	○	
		HDD暗号化	○	
		セキュアブート		○
	証拠保全方法の違いと使い分け	物理コピー	○	○
		論理コピー	○	○
		フォレンジックイメージ		○
	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	フォルダやファイルレベルでのデータ収集	○	○
コンピュータや補助記憶装置	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	○	○
	RAID	ハードウェアRAID、ソフトウェアRAID		○
		RAIDレベル		○
証拠保全媒体/取得保全データの管理	保管方法	電子機器/精密機器の観点からの留意点	○	○
		電子データの特性からみた留意点	○	○
		証拠データの保護（保全先の暗号化等）	○	○
	取得保全データの分析時における留意点			○
	媒体/データの所在/保管者変更に伴う留意点	CoC（Chain of Cusdody）	○	○
		CoCの役割	○	○
		CoCに求められる記載項目	○	○
証拠保全対象の多様化による問題	SSDの問題		○	○
	ハードディスクの大容量化問題		○	○
	クラウドサービスの問題			○
	その他の多様化問題		○	○
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	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	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	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	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		○	○

デジタル・フォレンンジック実務者資格(CDFP－P)シラバス案　＜技術系＞

大項目	中項目	小項目	CDFP-B(注1)	CDFP-P (注2)
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	タイムライン分析	○	○
		ファイル内容分析	○	○
	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	タイムスタンプ	○	○
		レジストリファイル	○	○
		イベントログ/システムログ	○	○
		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	文字コード	○	○
		キーワード検索(ブーリアン/正規表現/近傍)	○	○
	統計による分析のアプローチ			○
	人工知能の活用	教師データの学習と調査対象データのスコアリング	○	○
	代表的なデータ隠蔽(隠匿)方法	ファイル名変更		○
		拡張子偽装/削除		○
		データ記述改変による意図的な破損ファイル作成		○
		代替データストリームの悪用		○
		仮想ディスク内への格納		○
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	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		○	
	報告内容の補完目的とした関連データ/情報提出時の留意点			○
	第三者への委託による再調査/再鑑定	委託側の留意点		○
		受託側の留意点		○
デジタル・フォレンンジックにおける作業環境	フォレンジックラボ			○
	クラウドサービス上の作業環境			○
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暗号化の影響	HDD暗号化の種類(ツールで対応できるもの/できないもの)	○	○
		HDD暗号化設定の確認方法	○	○
		ファイル暗号化(EFS等)	○	○
	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	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	○	○
		リカバリパスワード等の代替手段		○
	目的を限定したファイルレベルでのデータ収集		○	○
	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	Windows環境におけるポイント	○	○
		Linux環境におけるポイント	○	○
		Mac環境におけるポイント	○	○

デジタル・フォレンンジック実務者資格(CDFP－P)シラバス案　＜技術系＞

大項目	中項目	小項目	CDFP-B(注1)	CDFP-P (注2)
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	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)の留意点	モデルの確認		○
		ロック解除方法(パスコード、パスワード、パターン、指紋、顔認証)の確認		○
		バックアップに関する情報(バックアップ先、バックアップパスワード)		○
		ケーブル接続の確認		○
		分析用コンピュータとモバイル端末間の通信可否の確認		○
		USBデバッグの設定確認		○
	モバイル・フォレンジックのデータ収集(証拠保全)手法	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		○	○
	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		○	○
	データベースファイルの分析	SQLite	○	○
		Realm Database		○
	クラウド上に残るモバイル端末のバックアップデータ		○	○
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	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	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	○	○
	ネットワーク・フォレンジックの対象	イーサネット	○	○
		TCP/IPプロトコル	○	○
		サーバソフトウェア	○	○
		アプリケーション層の通信プロトコル(DNS, HTTP, SMTP等)		○
		無線LAN		○
	ネットワーク・フォレンジックの基本的な流れ	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	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	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分析	○	○
	ファスト・フォレンジックが注目される背景・理由	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	揮発性情報のデータ収集と分析	○	○

デジタル・フォレンンジック実務者資格(CDFP－P)シラバス案　＜技術系＞

大項目	中項目	小項目	CDFP-B(注1)	CDFP-P (注2)
フォレンジックツール	証拠保全用ツール	フォレンジック専用証拠保全用ツールに求められる機能要件		○
		ハードウェア/ソフトウェアの特徴と留意点		○
		汎用ツールの適用		○
	分析/分析用ツール	フォレンジック専用分析/分析用ツールに求められる機能要件		○
		分析/分析対象のOSの違いによるツール選定の留意点		○
		汎用ツールの適用		○
ファイルシステム	パーティション	MBR,GPT		○
	ファイルシステムの機能	ジャーナリング		○
		スナップショット		○
	仮想ディスク	VHD/VHDX		○
		iso		○
		dmg		○
Windowsフォレンジック調査の実践	Windowsアーティファクト	レジストリ		○
		プリフェッチ		○
		イベントログ		○
		ファイル履歴		○
		プリントスプール		○
		サムネイルファイル		○
		ゴミ箱		○
		LNKファイル		○
		ジャンプリスト		○
	Windowsファイルシステム	NTFS		○
		FAT		○
		exFAT		○
		ReFS		○
		ボリュームシャドウコピー		○
LinuxやUNIX系OSフォレンジック調査の実践	Linux や UNIX 系OSのアーティファクト	サービス自動起動の仕組み(SysVinit, BSD init, Systemd)		○
		システムレベルの設定ファイル		○
		ユーザレベルの設定ファイル(ドットファイル)		○
		スケジュールによるコマンド実行(cron, at, systemd.timer)		○
		デスクトップ環境関連ファイル(XDG Base Directory Specification)		○
		各種ログ(ログファイル, Systemd ジャーナル)		○
		コマンドヒストリ		○
		プロセスファイルシステム(procfs)		○
	Linux や UNIX 系OSのファイルシステム	Btrfs		○
		ext4		○
		UFS		○
		XFS		○
		ZFS		○

デジタル・フォレンンジック実務者資格(CDFP－P)シラバス案　＜技術系＞

大項目	中項目	小項目	CDFP-B(注1)	CDFP-P (注2)
macOSフォレンジック調査の実践	macOSアーティファクト	Spotlight		○
		自動起動設定(launchd)		○
		Apple System Log (.asl)		○
		CoreAnalytics Files		○
		GateKeeper(QuarantineEvents)		○
		各種ログ(システムログ、アプリケーション)		○
		Apple独自ファイル形式(NSKeyedArchiver、Binary plist)		○
	macOSファイルシステム	APFS		○
		HFS+		○
	Mac環境における証拠保全	起動時のキーコンビネーション		○
		ターゲットディスクモード		○
		外部ディスクブート		○
		Startup Manager		○
		シングルユーザモード		○
	Mac環境におけるセキュリティ機能	FileVault1/FileVault2		○
		CoreStorage		○
		T2チップ		○
ブラウザ・フォレンジック調査の実践	閲覧履歴			○
	ブックマーク			○
	キャッシュ			○
	保存された認証情報			○
	Cookie			○
	設定情報	ブラウザの設定情報		○
		拡張機能の設定情報		○
	プライベートブラウジング			○
メモリ・フォレンジック調査の実践	メモリの内容の保存場所	RAM		○
		スワップ、ページファイル		○
		ハイバネーションファイル		○
	メモリダンプの取得方法	外部媒体への保存		○
		ネットワーク経由での保存		○
	メモリダンプに含まれる情報	プロセスの情報		○
		通信先の情報		○
		メモリに読み込まれたファイルの内容		○
		コードインジェクションされたマルウェア		○
クラウド・フォレンジック調査の実践	クラウドサービスの形態	IaaS		○
		IDaaS		○
		PaaS		○
		SaaS		○
		責任共有モデル		○
	クラウドサービスのデータ収集(証拠保全)	各サービス毎の手順		○
		物理コピー		○
		論理コピー		○

デジタル・フォレンンジック実務者資格(CDFP－P)シラバス案　＜技術系＞

大項目	中項目	小項目	CDFP-B(注1)	CDFP-P (注2)
サイバーセキュリティ分野におけるフォレンジック	サイバー攻撃手法	マルウェア感染(標的型メール攻撃、ドライブバイダウンロード, サプライチェーン攻撃等)		○
		ウェブアプリケーションに対する攻撃手法(SQLインジェクション、OSコマンドインジェクション, CSRF等)		○
		認証情報を使用した侵入(フィッシング、ブルートフォース攻撃、パスワードリスト攻撃等)		○
		ソフトウェアの脆弱性を悪用した侵入(リモートコード実行, 認証回避等)		○
		サービス不能攻撃		○
	セキュリティ侵害の痕跡(IoC)の発見	コンピュータ上のファイル検索(セキュリティソフト、YARA)		○
		セキュリティ機器(IDS,IPS)のログ		○
		ネットワーク機器、サーバの通信ログ		○
	セキュリティ侵害のタイムライン分析	コンピュータ内のタイムライン		○
		ネットワーク内のタイムライン		○
	マルウェア分析	表層分析・動的分析・静的分析手法の違い		○
		常駐・自動起動の方法		○
		マルウェア等の通信先		○
内部不正調査分野におけるフォレンジック	内部不正種別(大別)とその手法	不正会計		○
		品質不正		○
		情報流出(持ち出し)		○
		労務規定違反		○
		ハラスメント		○
	調査対象範囲の確定	調査対象者の選定		○
		調査対象デバイス／データの選定		○
		監視／管理ツール・ネットワーク機器ログの活用		○
	調査項目と不正との関連性	コンピュータ稼働状況分析に関する調査項目		○
		勤務・勤怠形態等、人的稼働状況分析に関する調査項目		○
		情報流出(持ち出し)に関する調査項目		○
		ファイル操作(アクセス)に関する調査項目		○
	アーティファクトが持つ情報	コンピュータ稼働状況分析に適用すべきアーティファクト		○
		勤務・勤怠形態等、人的稼働状況分析に適用すべきアーティファクト		○
		情報流出(持ち出し)調査に適用すべきアーティファクト		○
		ファイル操作(アクセス)調査に適用すべきアーティファクト		○
	コミュニケーションデータ分析	Eメールデータの調査		○
		チャットデータの調査		○

(注1)CDFP-Bで○が付いている項目はデジタル・フォレンジック基礎資格(CDFP-B)認定試験での出題範囲となります。
　　なお、デジタル・フォレンジック実務者資格(CDFP-P)認定試験シラバス検討に際してCDFP-Bの項目についても見直しを行っています。
(注2)CDFP-BとCDFP-Pの両方に○が付いている項目については、CDFP-Pでは、CDFP-Bよりも詳細な内容を出題します。