デジタル・フォレンジック資格認定
ワーキンググループ中間報告書

２０１９年4月２２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ワーキンググループ

１　目　的

２００４年８月にデジタル・フォレンジック研究会（以下「ＩＤＦ」という。）が発足して以来、第１６期目になる。その間、デジタル・フォレンジック（以下「ＤＦ」という。）は、法執行機関の捜査のみならず、企業における不祥事発生時の第三者委員会による調査、社員の不正行為に対する調査、米国での民事訴訟や行政調査における電子情報開示（ｅディスカバリ）及びサイバーセキュリティに係わるインシデント調査等、多方面にわたって活用が進んでいる。

一方、昨年２月に経済産業省より「情報セキュリティサービス基準」及び「情報セキュリティサービスに関する審査登録機関基準」が公表された[1]。
同基準は、「セキュリティ対策は、セキュリティ製品を購入しただけでは十分ではなく、事業者が行う情報セキュリティサービスの利用も含めて検討する必要があること」及び「専門知識をもたないサービス利用者が、サービス事業者の選定時にそのサービスの品質を判断することは容易ではないこと」を背景として、「情報セキュリティサービスについて一定の品質の維持向上が図られていることを第三者が客観的に判断し、その結果を台帳等でとりまとめて公開すること」が求められていることから、上記の二つの基準が策定された。

現在、デジタルフォレンジックサービス[2]についても審査基準に適合した企業がリストアップされＩＰＡから公表されている。上記基準において、「３　デジタルフォレンジックサービスに係る審査基準」の「（１）技術要件」の「ア　専門性を有する者の在籍状況」が掲げられている。同項において「デジタルフォレンジックサービスに従事する要員のうち、次のいずれかの要件を満たす者を技術責任者として業務に従事させる。」とあり、「(ア)　附則３－１に定める資格を有する者」が要件の一つとなっているが、その資格は、「情報処理安全確保支援士」又は「ＣＩＳＳＰ」である。しかし、同資格は必ずしもデジタル・フォレンジックに係る知識及び実務能力を問うものではない。

このような状況に鑑みて、ＤＦに係わる知識及び実務能力を公正かつ適正に評価し、認定するＤＦ資格認定制度が求められていると想定されることから、第１５期後半よりその開設に向けて「デジタル・フォレンジック資格認定ワーキンググループ（以下「WG」という。）」において検討を重ねてきたので、これまでの検討結果を中間報告する。

２　検討概要

第１５期のWGの活動として、米国での事例等を参考にしながらＤＦ資格認定制度について検討を行った。以下の４つの資料は、検討結果をまとめたものである。

①「ＤＦ資格認定制度骨子（案）」　　（別添１）
②「ＤＦ資格区分と要件項目（案）」　　（別添２）
③「ＲＡＣＩマトリックスと要件（案）」（別添３）
④「海外の資格認定ＣＦＣＥ」　　（別添４）

第１５期においては、ＤＦ資格認定制度のフレームワークを検討するとともに、受験者の学習範囲及び資格認定試験問題（以下「試験問題」という。）の出題範囲を特定する上で必要なシラバスを作成するため、「サイバーセキュリティ（インシデントレスポンスを含む。）調査」に関する職能分析を行い、要件項目を検討したところである。
第１６期には、「内部不正調査」及び「ｅディスカバリ」の職能分析と要件項目の調査を行い、上記３領域のシラバスを作成することとする。

---

[1]出典：経済産業省　http://www.meti.go.jp/press/2017/02/20180228002/20180228002.html
[2]情報セキュリティサービス基準において、「デジタルフォレンジック」と表記されていることから、このサービスについての記述ではこの表記を用いる。

WGにおける検討により、ＤＦ資格については、上級、中級及び初級（仮称：名称は今後検討する。）とするが、シラバス及び試験問題の作成に当たって、初級・中級・上級に積み上げる方式、所謂「富士山型」では、実用的な試験問題を構成しにくいことが分かった。

その結果、初級の資格試験問題は、ＤＦの基礎的な理解を評価するものとし、上記３領域に共通する設問とすることとした。

中級・上級の試験問題は、各領域の設問とする所謂「八ヶ岳型」にすることとした。第１６期では、八ヶ岳型で、「ＤＦ資格区分と要件項目」を見直し、それに合わせて「ＲＡＣＩマトリックスと　要件」を適宜修正して確認し、その結果を踏まえてシラバスを作成するとともに、「ＤＦ資格認定制度骨子」を修正して仕上げることとする。

３　調査及び職能分析

別添１「ＤＦ資格認定制度骨子（案）」及び別添２「ＤＦ資格区分と要件項目（案）」の作成に当たり、ＣＦＣＥ（Certified Forensic Computer Examiner Program）等の米国のＤＦ資格認定についての調査及びＤＦ業務に携わる実務者像、職務領域に応じた業務と職位構成についての職能分析を行なった。

（１）　米国のＤＦ資格認定状況の調査

ＣＦＣＥの運営組織は、非営利団体の国際コンピュータ捜査スペシャリスト協会（IACIS:The International Association of Computer Investigative Specialists）であり、米国等において権威のある組織である。なお、正会員資格を得られるのは、法執行機関及び政府の現職員・元職員並びに政府機関の契約職員に限定されている。ＣＦＣＥの認定は、非会員にも適用される。

ＣＦＣＥ受験に当たって、ＩＡＣＩＳは基礎コンピュータ・フォレンジック調査官（BCFE:Basic Computer Forensics Examiner）のトレーニングコースを準備している。
ＢＣＦＥは、１０日間、７６時間のフォレンジック習得コースであり、受講料は２，９９５ドルである。
ＢＣＦＥの受講に代えて外部でのプログラムも用意されており受講料は７５０ドルである。

ＣＦＣＥの認定試験は、Peer Review と認定試験の２つのフェーズで構成されている。
Peer Review は、３０日以内に実務問題４問に合格する必要がある。また、受験者には学習を進めるためのコーチが割り当てられる。これに合格すると認定試験を受けることができる。

認定試験では、受験者はハードディスクの実務問題を４０日以内に、知識ベースの設問１００問を１４日以内に解かなければならない。８０％以上の得点を取ればＣＦＣＥとして認定される。

ＣＦＣＥの有効期間は３年間である。再認定を受ける前に４０時間の継続教育を受講する必要がある。

米国のＤＦ資格認定は、時間と費用が掛かるが、国内でＤＦ認定制度を開設するに当たって試験時間及び受験料について考慮する必要がある。
（別添４「海外の資格認定ＣＦＣＥ」参照）

（２）　職能分析

実務者像の検討においては、まず民間組織にみられるＤＦ業務の実態をＫＳＡＯ（Knowledge：知識、Skill：技術、Ability：能力、Other characteristics：その他、価値観／経験値など）の観点から情報収集を実施した。

収集された情報は、「ＤＦ分野の専門家」（Subject Matter Expert）からなるＷＧの議論を経て、「サイバーセキュリティ調査」、「内部不正調査」、「ｅディスカバリ」の三領域にわたることが特定された。

今回はこれら領域のうち、サイバーセキュリティ調査に焦点をあて、この領域における実務者の「業務仕様書」（Scope of Work）について検討を進めた。

その検討において、サイバーセキュリティ調査に従事するＤＦ人材においては、職務だけでなくその職務に付随する責任（Accountability）を明確にすべきとの議論がなされた。そこで、責任、権限レベルを明示するための区分として、「マネージャ」、「リーダー」、「アナリスト」の職位（position）を設定した。

これら三つの職位に位置付けされているＤＦ人材が対応する業務範囲と職務を構成する最少要素であるタスクについて整理を行なった。

タスク遂行のために必要となるＫＳＡＯ要件については、「サイバーセキュリティ人材育成スキーム策定共同プロジェクト」公表の「総合セキュリティ人材モデル」に定義されるフォレンジックエンジニア職種ならびに、「日本ネットワークセキュリティ協会」公表の「情報セキュリティ知識項目（SecBoK2019）」に定義されるフォレンジックエンジニアの各項目を参照し、それぞれのタスクに対して要件の割り当てを行った。その上で、「ＲＡＣＩ（レイシー）チャート」の方法を用いて、職位における責任と権限を明確に区分した。これにより、各職位における「実行責任（Responsible）」、「説明責任（Accountable）」、「相談対応（Consult）」、「情報提供（Inform）」を明らかにするに至った。なお、検討結果の詳細については、別添３「ＲＡＣＩマトリックスと要件（案）」のチャートにまとめた。

４　第１６期の検討課題

（１）第１５期は「サイバーセキュリティ調査」の職能分析を行ったが、第１６期は「内部不正調査」及び「ｅディスカバリ」についても職能分析を行い「ＤＦ資格区分と要件項目」及び「ＲＡＣＩマトリックスと要件」を改善し、その結果を踏まえて各領域のシラバスを作成する。

（２）シラバスに基づき模擬試験問題を作成し、９月のＩＤＦトレーニングにおいて模擬試験を実施する。

（３）設問試験に関して、ＣＢＴによる試験方法を検討する。

（４）実技を伴う試験に関しては、第１６期中に検討を進め実施方法を示す。

（５）「ＤＦ資格認定制度」の最終報告書を作成する。

（別添１）

ＤＦ資格認定制度骨子（案）

１　ＤＦ資格認定対象者（受験者）

ＤＦ資格認定制度において、主たる対象者は、以下の業務に携わる者、今後携わる予定の者及びＤＦに関する知識・実務能力に関する評価を得ようとする者等を想定している。

（１）　上級・中級資格試験

① リーガルテクノロジーを業態とする企業のＤＦ従事者等
② インシデントレスポンスを業態とする企業のＤＦ従事者等
③ 一般企業のＤＦ業務に従事する者及びその候補者（以下「ＤＦ従事者等」という。）
④ 監査法人関係者のうちＤＦに関する知識を必要とする者
⑤ 法曹関係者のうちＤＦに関する知識を必要とする者
⑥ 法執行機関等、官公庁のＤＦ従事者等
⑦ その他、上級・中級資格を得ようとする者

（２）　初級資格試験

① ＤＦについて基礎的知識を得ようとする者
② 上位の資格を取得しようとする者

２　ＤＦ資格認定制度のフレームワーク

（１）　ＤＦ資格認定試験制度の方向性

① ＤＦ資格認定試験は、ＩＤＦ定款第５条「（８）デジタル・フォレンジック技術認定事業」に基づくＩＤＦの事業として実施する。

② 試験問題の作成及び採点を行うため、ＤＦ資格認定試験実施委員会（仮称、以下「委員会」という。）を設置する。委員会は、ＩＤＦ理事会が指名する委員長及び委員長が指名する複数名の委員にて構成する。

③ 受験料は、受験し易いようＩＰＡの情報処理技術者試験の受験料程度が望ましいが、資格認定制度の継続性に関しても考慮する必要があることから、数千円～数万円の範囲とする。

④ ＤＦ及びＤＦの対象は、技術革新のスピードが速い分野であることから、ＤＦ資格の有効期間（２年間又は３年間）を定め、ＤＦ資格の更新に必要な要件を定める。

（２）　ＤＦ資格認定試験の区分（仮）

ＤＦ資格認定試験は、次の試験区分にて実施する。

① 上級試験：ＤＦに関する知識・実務能力・指導力及びＤＦの実施結果に対する説明能力について評価する。
② 中級試験：ＤＦのプロセス及び対象機器の取扱いに関する知識・実務能力を評価する。
③ 初級試験：ＤＦに関する基礎知識を具備しているか評価する。

（３）　試験形式

① ＤＦに関する知識を問う設問（選択式）
② 実技試験

（4）　試験実施方法

①　受験資格

上級及び中級試験は、初級試験合格者が受験できることとする。初級試験は、委員会が実施する講習会の終了者が受験できることとする。

②　上級及び中級試験

１次試験として設問試験（選択式）を実施する。設問試験の採点結果が８０点以上を１次試験の合格者とする。２次試験は、１次試験の合格者に対して実技試験を実施する。

設問試験は、オンライン又は試験場においてＣＢＴ（Computer Based Testing）により数時間の試験を実施する。

実技試験は、委員会が証拠保全対象のハードディスクを準備し、試験時間中は当該ハードディスクを受験者に貸与する。受験者は、与えられた期間内に当該ハード　ディスクに対して、証拠保全及び解析を実施し、解析結果の報告書を作成するとともに、一連のプロセスの実施記録を作成し委員会に提出する。

委員会は報告書及びプロセスの実施記録を基に採点を行い合否を判定する。
なお、ＩＤＦ理事会が認定した企業の特定の研修コースを実技試験に変えることができる。

③　初級試験

ＤＦの基礎知識が得られるよう、数日間の講習会を実施することを前提とする。講習会の最終日に講習会の内容に関する設問試験を実施して、８０％以上の得点を取れば合格とする。

（5）　参考図書

①　学習のため次に掲げる参考図書を推薦する。

「基礎から学ぶデジタル・フォレンジック」
安冨潔・上原哲太郎　編著、日科技連出版、２０１９年

「証拠保全ガイドライン　第７版」
ＩＤＦ「証拠保全ガイドライン」改訂ワーキンググループ、２０１８年

「デジタル・フォレンジックの基礎と実践」
佐々木良一　編著、東京電機大学出版局、２０１７年

「デジタル・フォレンジック概論」
羽室英太郎・國浦淳　編著、東京法令出版、２０１５年

「改訂版デジタル・フォレンジック事典」
佐々木良一　監修、舟橋信・安冨潔　編集責任、日科技連出版、２０１４年

②　受験のための問題集の出版は、試験を重ねた後に検討する。

「ＤＦ資格認定」WGメンバー一覧（所属は２０１９年４月現在）

座　　長：舟橋　信（ＩＤＦ理事、株式会社 FRONTEO　取締役、株式会社セキュリティ工学研究所　取締役）

メンバー：安冨　潔（ＩＤＦ会長、京都産業大学　法学部　客員教授、慶應義塾大学　名誉教授、弁護士）

上原　哲太郎（ＩＤＦ副会長、立命館大学　情報理工学部　教授）

佐藤　慶浩（ＩＤＦ副会長、オフィス四々十六　代表）

名和　利男（ＩＤＦ理事、株式会社サイバーディフェンス研究所　専務理事　上級分析官）

櫻庭　信之（ＩＤＦ理事、シティユーワ法律事務所　パートナー弁護士）

河原　徹（株式会社 FRONTEO　クライアントテクノロジー部　フィールドサポートテクノロジー課）

大徳　達也（株式会社サイバーディフェンス研究所　情報分析部　部長／上級分析官）

青嶋　信仁（株式会社ディアイティ　セキュリティサービス事業部　事業部長）

清水　智（トレンドマイクロ株式会社　執行役員　公共ビジネス戦略推進室　室長）

林　憲明（トレンドマイクロ株式会社　公共ビジネス戦略推進室
プリンシパルセキュリティアナリスト）

野本　靖之（ＩＤＦオブザーバー）

鳥飼　貞一（ＩＤＦオブザーバー）

以上