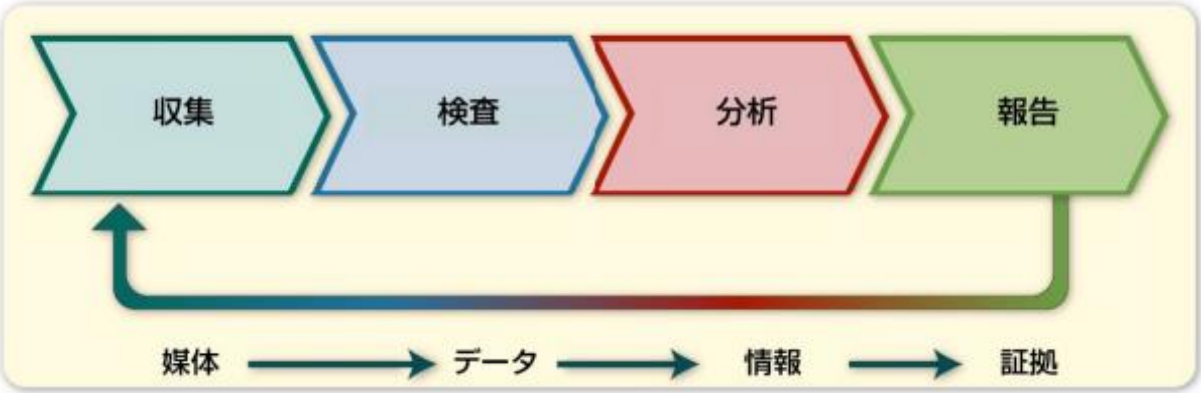
実務家から見たDFベンダー選定のポイント

前回ご紹介した証拠保全ガイドラインとデジタル・フォレンジック・プロフェショナル認定（Certified Digital Forensic Professional）を踏まえ、デジタル・フォレンジック調査会社（以下、「DFベンダー」といいます。）に支援を受ける側から見たDFベンダー選定のポイントについて検討します。

DFのプロセス

DFベンダー選定にあたり、DFベンダーに依頼するDFプロセスを理解する必要があります。

DFプロセスには多くのモデル（注1）がありますが、各モデルは、フェーズの細分化レベルや個々のフェーズで使われる用語などが少しずつ異なるものの、基本原則や全体的な方法論は同一です。DFプロセスの基本フェーズは、①「収集」、②「検査」、③「分析」、④「報告」で構成され（注2）、DFはこれらのプロセスを経て「媒体」から「証拠」への変換を行う技術とも言えます。



（出典：NIST SP800-86日本語訳「インシデント対応へのフォレンジック技法の統合に関するガイド」図3-1. より転載）

ここで押さえておきたいポイントは、DFプロセスのうち、膨大なデータを扱う左側のフェーズが主にIT系の作業領域で、フローが進むにつれて、法務的な作業領域となるという点です。DFベンダーと一口に言ってもそれぞれ得意領域があり、DFプロセスの中で効果的な支援を提供できる領域が異なるという点を理解することが、適切なDFベンダー選定の第一歩といえます。特定非営利活動法人デジタル・フォレンジック研究会の団体会員について掲載されている「製品・サービス区分リスト」（注３）を見ると、フォレンジックツールの開発、データ復旧、画像解析などそれぞれの分野における高い技術力を持つ会社や、弊社と同様に調査実務に精通し、調査活動に関するコンサルティング機能を持つ会社など、各社の特徴が表れています。

（注１）例えば、eDiscovery（eディスカバリー、電子情報開示）を行う際のワークフローのデファクトスタンダードといえるEDRM （The Electronic Discovery Reference Model：電子情報開示参考モデル）などが挙げられます。（参考：https://www.fss.jp/edrm/）

（注２）DFプロセスの詳細については、弊社コラム（https://legalex.co.jp/column/）#11から#13および拙稿「金融機関の不祥事対策におけるデジタル・フォレンジックの活用」（金融法務事情 2020年6月25日号 No2140 21頁以下）をご参照ください。なお、当該モデルにおいて、いわゆる「データの保全」は「収集」に含まれます。

（注３）https://digitalforensic.jp/wp-content/uploads/2020/09/product_service-v.6.pdf

DFベンダー選定のポイント

DFベンダーには、情報技術やDFの技術的な内容は当然のこと、DF実務経験や法執行機関による捜査、日米の訴訟制度や実務に関する知識や理解も求められます（注４）。これらを有していることを前提にしたうえで、DF調査の発注に当たっては、DFベンダーの特徴と以下の要素を考慮して、DFベンダーを選定することになります。

１．事案の性質

例えば、機密情報の漏えい事件であれば、一般的にメールやチャットデータなどのみならず、メモリ上のデータなどの揮発性情報調査やレジストリ調査、システムファイル調査の重要性が高まることから、これらのデータを効率的に解析し、解釈できる技術力が重視されます。

訴訟に至ることが予想されるケースでは、証拠力の保持が重要となるため、DF実務経験が豊富で、CoC（Chain of Custody：証拠保全の一貫性）を適切に保持、立証できるDFベンダーに依頼することが必要です。加えて、国際的な事案においては、関係国において国際的なネットワークを有しており、e-Discovery（米国民事訴訟手続における電子データ開示手続）やGDPR（EU一般データ保護規則）など各国のレギュレーションに対応できることが重要なポイントになります。

上場企業における会計不正では、限られた期限で調査を行う必要が生じるため、迅速で柔軟な対応や調査主体に対し必要な提言ができることが重要になります。また、会計不正のうち粉飾など高度な会計的判断が必要となる事案では、1次的なドキュメントレビューの段階で会計的知見が必要となる場合もあります。

２．人的リソース

DF調査は突発的に発生しますが、 DF調査への備えを平時から行っている組織は少ないことから、調査に対応できるリソース（時間やノウハウなど）を有する人材が乏しいことが一般的です。例えば、調査ノウハウに不安がある場合や、専門的又は多面的な視点での調査が必要な場合などは、コンサルテーションを伴ったDF調査の支援が受けられるかどうかを重視すべきでしょう。また、時間的制約や事案の広範さなどから調査リソースが不足する場合には、調査補助者やドキュメントレビュアー等を提供してもらえるかどうかも重要な要素となります。

３．コスト

DF調査に掛けられるコストも重要な考慮要素です。DFベンダーによって課金体系や単価は異なります。どうしても時間が無い場合を除き、保全対象機器や依頼する業務範囲などについて同一の前提を提示して複数のDFベンダーの見積を取得することが推奨されます。その場合、コストは安ければよいというものではないため、見積りの前提などが明確になるように、見積書への根拠の記載やそれとは別に簡易な提案書の提示を要請すること、見積の内容について説明を受ける機会を設けることが望ましいと考えられます。

（注４）前回ご紹介した特定非営利活動法人デジタル・フォレンジック研究会が実施するデジタル・フォレンジック・プロフェショナル認定（Certified Digital Forensic Professional）においても同様のスキルが求められています。

問題となりやすいケース

弊社の経験上、DFベンダーとの間で問題となりやすいケースとして、①コストを重視してDFベンダーを選定した結果、依頼側としては「伝達した事案概要や調査方針、DFプロセスでの検出事項を踏まえて適時に提案や相談をしてくれるだろう」と考える一方で、DFベンダー側としては「依頼事項に含まれていないため実施していない」といった期待ギャップが生じたケースや、②発注時にDF調査コストを精緻に見積もることはできない点は理解していたものの、調査中にDFベンダーから適時のコスト報告がなされず、完了時に想定を大きく超える請求書が送られてきたケースが挙げられます。

これらは相互の業務理解が不十分であったことや、業務中の連携が不十分であったことに起因します。このように選定後もDFベンダーに任せきりにしないこともまた重要ですので、調査中における状況変化や進展に応じて、適時かつ柔軟な連携を取ることができるベンダーであるかどうかも、選定時のポイントの一つになるでしょう。

本件に関するお問い合わせ

リーガレックス合同会社
大阪事務所　業務執行社員　公認会計士／公認不正検査士／公認情報システム監査人
立川　正人（masato.tachikawa@legalex.co.jp）
東京事務所　業務執行社員　公認会計士／税理士／中小企業診断士
髙山　清子（sumiko.takayama@legalex.co.jp）

発行会社

会社名	リーガレックス合同会社（LEGALEX LLC）
代表社員	深山　治（公認不正検査士）
事業概要	LEGALEX（Legal + Expand）をコーポレートコンセプトとして、法務領域に関連するテクノロジーと公認会計士・税理士の専門性を、企業内外の法律専門家や会計専門家等に提供し、拡大する業務領域への対応を支援することを目的としている。東京・大阪・福岡を拠点に、デジタル・フォレンジックスについての高い技術と知識、会計税務に関する見識を融合させ、国内外の不正調査や内部監査等に関する数多くの支援実績を有する。
所在地	［東京］　東京都中央区銀座1-16-7　銀座大栄ビル ［大阪］　大阪府大阪市淀川区宮原1-1-1　阪急新大阪ビル ［福岡］　福岡県福岡市博多区博多駅東2-5-19　サンライフ第３ビル
HP	https://legalex.co.jp