デジタルフォレンジック

Digital Forensic

KPMGは、情報漏洩、不正会計、横領・窃盗等の不正・不祥事の調査、およびe-Discoveryにおいて、デジタルデータの保全・復元・解析を行うサービス（デジタルフォレンジックサービス）を提供します。デジタルフォレンジックの専門家が、コンピュータ・システムに保存されているデータの証拠能力を保全しながら収集・復元した上で、事案に応じたデータ解析を行い、事実解明を支援します。

また、技術的な支援だけではなく、豊富な知識・経験にもとづき、調査プロセスの立案・管理に係るアドバイスも提供します。

今日の企業活動において、電子メールや電子文書の利用は必要不可欠となり、日常コミュニケーションから機密情報まで、色々な情報がコンピュータ・システムに保存されるようになりました。また、電子メールや電子文書だけでなく、電子メールの送受信履歴や電子決裁システム上の承認履歴等、色々な履歴が、これまで以上にデジタルデータとして記録されるようになりました。

このような背景から、コンピュータ・システムに残された情報をもとに、不正や不祥事の実態を解明しようとする動きは強まっており、不正アクセスや情報漏洩などのコンピュータ犯罪だけでなく、従業員による横領事件やインサイダー取引、経営者による粉飾決算など、色々な調査においてデジタルフォレンジックの重要性が注目されています。

一方で、デジタルデータには消失しやすく改ざんされやすい性質があるため、それが法廷において証拠能力を持ち、行為者の特定に寄与するか否かは、調査の手順、客観性などさまざまな要素に依存することとなります。実際に、証拠保全の手順を踏まずに内々で調査を行ったために、証拠となるデータを喪失してしまう、データの証拠能力を無くしてしまうという事態になることは少なくありません。真相を究明し、証拠能力を最大限維持し、係争に備えるためには、専門家による調査やサポートが必要不可欠となります。

デジタルフォレンジックの主なサービス

具体的な、サービス内容については、不正事案の内容や調査要件をお聞きした上でご提案します。

計画・準備	■ 調査目的を把握し、調査対象となる人物・情報機器等を特定します。 ■ 証拠隠蔽やプライバシー侵害等のリスクを考慮した上で、効果的・効率的な調査ができるように調査計画を立案します。
データ収集・保全	■ データベース、ファイルサーバ、メールサーバ、パーソナルコンピュータ、携帯電話、スマートフォン、USBメモリ等の各種電子媒体から調査対象データを取得します。 ■ 調査対象データの取得は、フォレンジック専用ツールを用いて証拠能力を保全しながら実施します。
データ復元・加工	■ 削除された電子データを復元します（携帯電話、スマートフォンのデータ復元も対応可能です）。 ■ 必要に応じてパスワード付ファイルの解析を試みます。 ■ データ加工を行い、フォレンジック専用の検索・分析用ツール等へデータを格納します。
データ検索・分析	■ フォレンジック専用の検索・分析ツール等を用いて電子文書、電子メール、業務システムデータ等を調査し、事実解明を行います。 ■ 調査目的に応じて犯行者・協力者の特定、犯行動機の解明、余罪の追及等を行います。
報告書作成	■ 分析結果をもとに、事実関係を整理し、報告書を作成します。 ■ 調査対象とした組織・人・機器・期間、調査に使用した製品・ソフトウェア、実施した調査手続の内容、分析結果から得られた情報等を正確に記載し、信頼性の高い報告書を提示します。

計画・準備

調査目的を把握し、調査対象となる人物・機器を特定し、会社のルール、ポリシーを確認した上で、調査計画の立案および調査機器等の準備を行います。

不正・不祥事の調査は、限られた時間で行うため、やり直しが困難な手続きが多数を占めます。このため、調査計画は綿密に立てておくことが望ましいと言えます。また、調査の初期段階においては不確定要素が多いため、不測の事態にも柔軟に対応できる調査計画である必要があります。

調査対象となる機器の設置場所、物理的セキュリティの有無、ネットワーク接続の可否や、調査対象機器の詳細情報等を事前に確認し、これらに応じた調査機器を準備します。最近のコンピュータでは、指紋認証や暗号化が施されているケースが増えているため、事前に対応手順を整えておく必要もあります。

調査計画の立案	✓ 調査対象者に対するプライバシー侵害等のリスクを考慮し、従業員規定などを事前に確認します。 ✓ 調査対象者が非協力的であったり、証拠を隠蔽したりする可能性を考慮し、調査を行うタイミングや順序を検討します。
調査機器等の準備	✓ 調査対象機器に到達するまでのセキュリティ、および調査対象機器自体のセキュリティがどのように施されているか確認し、事前に解除する手順を整えます。 ✓ 調査対象機器の詳細情報を事前に入手し、それに応じた調査用機器を準備します。

データ収集・保全

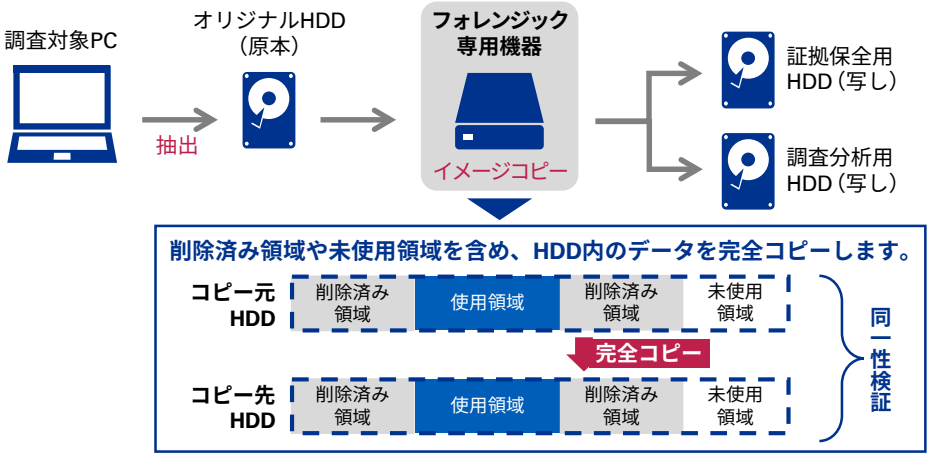
パーソナルコンピュータ、ファイルサーバ、電子メールサーバ、業務システムサーバ、携帯電話、スマートフォン等に格納されているデジタル・データの証拠能力を失わないよう収集し、保全します。

デジタル・データには毀損しやすく改ざんしやすい性質があるため、適切な手続のもと、デジタルフォレンジックの専用機器や専用ソフトウェア等を利用して収集し、保全することが望ましいと言えます。データ保全を適切に行わないと、訴訟において証拠能力が認められないリスクが高まります。「収集したデータから有用な情報が得られたが、証拠として認められなかった」という事態を避けるために、データ保全は確実に行う必要があります。

KPMGは、米国、英国などフォレンジック先進国における実績に裏打ちされたノウハウを駆使し、デジタル・データを迅速かつ安全に収集・保全します。また、さまざまな調査環境に応じて柔軟かつ適切にデータ取得ができるよう、各種専用機器および専用ソフトウェアを保有しています。

データ保全	✓ 調査対象機器内のHDDをイメージコピー（完全コピー）し、証拠保全用と調査分析用のHDDを作成します。 ✓ オリジナルHDD（原本）と証拠保全用HDD（写し）の同一性検証を行います（案件に応じて、バイナリ・コンペアやハッシュ値・コンペア等を行います）。 ✓ フォレンジック専用のイメージコピー機器を使用することで、原本への書き込み（改ざん）を防止した状態でコピーを取得します。 ✓ 削除済み領域を含めてコピーするため、削除済みデータの復元を試みることができます。

パーソナルコンピュータのデータ保全イメージ



データ復元・加工

不正に関する情報は、通常、意図的に隠蔽されています。そのため、削除された電子文書や電子メールを復元※し、隠蔽された情報を調査することは、デジタル・フォレンジックを導入する大きなメリットであるといえます。KPMGは、状況に応じて適切な復元ツールを駆使し、削除されたデータの復元を試みます。また、限られた期間で膨大なデータを効率的に分析するためには、調査要件に応じたデータ加工が必要となる場合があります。具体的には、複数人の電子メールに対して高度な検索・分析を行う必要がある場合、柔軟かつ高速に検索・分析できるように、電子メールデータを加工し、分析用DBに格納したりします。

データ復元	✓ 削除されたWord、Excel、一太郎、PDF等の電子文書の復元を試みます。 ✓ Outlook、Outlook Express等の電子メールソフト上で削除されたメールデータの復元を試みます。
データ加工	✓ 各種セキュリティ製品やOSに収録されているデータ（ネットワークアクセス履歴、PC操作履歴、電子メールアーカイブ等）を検索・閲覧できる状態にします。 ✓ バックアップテープに収められた電子文書や電子メール等を検索・閲覧できる状態にします。 ✓ 圧縮ファイルを解凍し、検索・閲覧できる状態にします。 ✓ 必要に応じて、パスワードロック付ファイルのパスワード解除を試みます。

※ 既に新しいデータで上書きされている場合等、データの状態によっては復元できない場合があります。

データ検索・分析

大量データの中から証拠となり得る情報を見つけ出すためには、コンピュータの中にあるさまざまな情報を有効かつ効率的に検索・分析する必要があります。

例えば、大量のデータを特定キーワードや特定期間で絞り込んだり、ファイルの最終更新日時や電子メールの送受信日時等で時系列に分析し、電子メールの送受信アドレス・頻度から交友関係を洗い出したり、調査目的に応じた柔軟かつ迅速な検索・分析を行う必要があります。

KPMGは、不正調査に特化した検索・分析ツールを複数保有しており、調査目的に応じた検索・分析を素早く進めることができます。また、国内外問わず数多くの調査実績があるため、調査目的に応じて、効率的かつ効果的な検索・分析を、柔軟に行うことができます。

また、e-Discoveryのレビューを行う際のシステム環境の提供も行います。レビューツールは、ご要望に応じて柔軟に対応することが可能です。

検索・分析	✓ 電子文書や電子メールの検索を行う場合、取扱いが可能な電子文書の種類（Word、Excel、PDF、一太郎等）、電子メールの種類（Outlook、Outlook Express、Lotus Notes、Thunderbird等）、および文字コード（SJIS、UTF8、UNICODE等）を考慮してツールを選定します。 ✓ 全文検索を行う際、検索速度を優先する形態素解析方式を採用するか、検索精度を優先するN-Gram方式を採用するか、その他方式を採用するか等、案件の内容に応じて検索方式を選定します。

報告書作成

分析結果をもとに事実関係を整理し、報告書を作成します。調査対象とした組織・人・機器・期間、調査に使用した製品・ソフトウェア、実施した調査手続の内容、分析結果から得られた情報等を正確に記載し、信頼性の高い報告書をご提供します。

株式会社 KPMG FAS
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ ノースタワー
T: 03-3548-5770
E: fasmktg@jp.kpmg.com
home.kpmg/jp/fas