Computer Forensics Service

コンピュータ・フォレンジックサービス

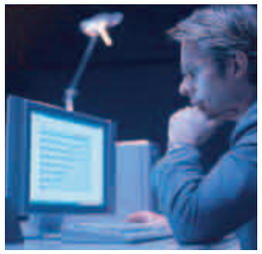
フォレンジック(Forensics)とは、科学捜査や鑑識という意味の言葉です。コンピュータ・フォレンジック(Computer Forensics) とは、情報漏洩事件、犯罪、訴訟等の際に関係するデジタルデータを専門の手法やツールによって調査・分析し、法的証拠性を明らかにする、いわば「デジタル鑑識」ともいうべきものです。

情報漏洩やPC不正使用の調査 / 分析

コンピュータ・フォレンジックサービスはデータの改竄、削除などにより既存のツールでは証拠を検出することが困難な被害を受けたデジタルデータについて、高度な専門ツールによって調査分析することにより、不正行為の追跡を行い、膨大なデータの中から決定的な証拠の発見をお手伝い致します。

長年の経験を持つデータ復活サービスの技術を基に、専門のスタッフがコンピュータ・フォレンジックの作業を行います。

- ○ 企業情報の漏洩　顧客リスト、社外秘等の流出の有無
- ○ 不正ダウンロード　アクセス禁止のサーバからの内部情報の持ち出しの有無
- ○ データの改竄　証拠隠滅のためのデータ消去の実行有無
- ○ コンピュータの私的利用　業務以外の利用痕跡の有無



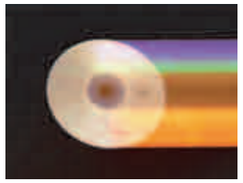
インシデント解決の為の適切なフォレンジック調査

内部での行動が疑わしい、また不正が発生してしまった場合はその後の対応のためにも、詳細な事実関係を素早く的確に調査することが何よりも重要です。さらに組織内の関係者以外に疑惑や焦燥感を起こさせずに公正なフォレンジック調査を行うことが解決への一番の対策になります。

現代社会の背景

ある統計資料では全犯罪を内部犯罪(身内や従業員などが起こす犯罪)と外部犯罪(被害者(社)と加害者(社)とが全く関係がない、もしくはあっても犯罪発生のトリガーになるほどの因果関係がない犯罪)に分けると何と８割近くが内部犯罪に分類されます。

しかしながら、日本というカルチャーは世界でも珍しいほどセキュリティという概念が希薄で、万一内部犯行と判った場合にはそっと絨毯の下にゴミを覆い隠すように隠蔽してしまいがちです。私どものフォレンジック調査とは一言でいうなら「デジタル鑑識」と考えて下されば、近いイメージになると思います。



昨今、「不正調査」におけるフォレンジック調査の利用は確実に増加しております。ただし、他の犯罪に比べまだまだ扱いが軽いのが「情報セキュリティ犯罪」です。

例えば、売上100万円を使い込んだ場合では解雇事由として８割近く(77.9%)に達しているものの、社外秘の重要機密情報を漏洩させた場合では66%、コンピュータ上のデータやプログラムを改竄した場合では更に27%に留まっており、これは論理的、倫理的に問題ありと考えざるを得ません(数値は財団法人労務行政研究所調べ)。情報ファイル漏洩が売上100万円より低い解雇事由になっていることは、専門家として「恥ずかしい」気持ちになります。

この様な現代社会の背景の基、フォレンジック調査を退職者パソコン調査というニーズに合わせメニューの拡充を行うなど、時代に沿ったフォレンジック調査の方向性にも目を向けながら活動しております。

デジタルデータの複雑性

デジタルデータは大変揮発性の高いデータです。例えば事件などを調査するために、専門的な処置をせずパソコンの電源を入れてしまうと、OSの立ち上げの際に自動的に数百ものファイルが更新されてしまいます。これによりパソコンの最終ログイン日等が変更され事件発生後の証拠改竄の可能性の余地を残してしまいます。

現在のデジタルデータ(PC等)は十数年前のデータとはその形式が変わってきており、調査する際そのデータを見れば全てが簡単に分かるというわけにはいきません。Windows・Macなど使用者が便利になる一方、データ自体はどんどん複雑化しています。パスワードが掛かっているファイルもあります。また、レジストリなどといった通常のPC操作ではあまり目にしないようなデータに対しても解析していくことが、コンピュータ・フォレンジックでは重要な作業です。

弊社ではこれに対し、しっかりとした知識と技術を持った者が作業にあたり、御社の企業情報漏洩や不正利用等を調査し、訴訟を含め全面的に支援いたします。

保管の継続性の証明

コンピュータ・フォレンジック調査を行う場合、裁判所など法的機関で証拠能力を証明するため、保管の継続性(Chain of Custody)に注意することが要求されます。

保管の継続性とは、証拠として提出されるデータが常に同一のものであり、調査の過程においてデータの改竄を行っていないことを証明していくことです。例えば、証拠となるハードディスクを現場で取得し当社のフォレンジック・ラボに持ち帰り、調査・解析を行い報告書をまとめ法廷に提出したとしても、それだけでは現場から当社までの輸送時に別のものに入れ替わった可能性は否定できません。さらに証拠として提出するデータに関しても改竄の可能性を否定できません。その問題を解決するため Chain of Custody認証(CoC認証)が存在します。

当社はCoC認証を実現するため、証拠となるデータの移動をする毎に必ずハッシュ値を取ることにより、そのデータの証拠性を保証しております。ハッシュ値とは、あるデータをハッシュ関数を通すことによって得られる値であり、そのデータを少しでも書き換えてしまうと得られるハッシュ値は全く違うものになってしまいます。それゆえに移動前のデータと移動後のデータのハッシュ値を比較し、一致することを確認することによってデータの同一性を確認します。主に使われるハッシュ関数はMD5、SHA-1といった関数が存在します。

今までの調査例

退職者/異動者パソコン調査

→これは法人契約で年間契約(台数制限なし)、もしくは月１０台や５台等の台数固定契約となります。いずれも原則は年間契約となります。ここでの反響はすごいものがあり、従業員に報知することで内部漏洩事故、事件が激減した企業様もございます。

Winny利用痕跡調査

→これは従業員のパソコン(会社内かご自宅のパソコン)を調査して Winnyの利用があったのか？ あったならそれは何年前なのか？また、ウイルスに感染されたのかなどなど企業側にとっては極めて重要な判断材料に繋がるものです。

メール内容調査

→時間指定、宛先指定、添付ファイル有無指定、削除メール指定・・・そしてフォレンジック固有な作業としてはキーワード指定も実行可能(例えば、全メールで「社外秘」という単語があるメールのみチェックする)です。

Computer Forensics Service