



ネットエージェント株式会社
フォレンジック調査部

『フォレンジック調査サービス』

～ご依頼から、ご報告までの流れ～

(1) フォレンジック調査概要

ネットエージェントでは、コンピュータ・フォレンジック手法を利用した調査サービスをご提供しております。フォレンジック調査サービスをご利用いただくことで、パソコンのハードディスクに記録されているデジタル・データの保全(複製)、デジタル・データの解析など専門的な調査¹が可能になります。

(2) 調査ご依頼前に

フォレンジック調査をご依頼いただくには、調査対象機器(例:パソコン・外付けHDD・USBメモリなど)の所有者・使用者との間で、デジタル・データの調査実施に関して、事前に同意を得ていただく必要があります。

会社が所有している機器であっても、機器の使用者との間で就業規則などにより調査の実施が明確になっていない場合には、「フォレンジック調査 同意書(複製・調査)」のような同意書を、機器の使用者様とご確認いただき、調査への同意(署名・捺印)を得ていただく必要があります。

事前の同意なくフォレンジック調査を実施することで発生するリスクに関しては、法律の専門家(弁護士)などにまずはご相談ください。

調査への同意

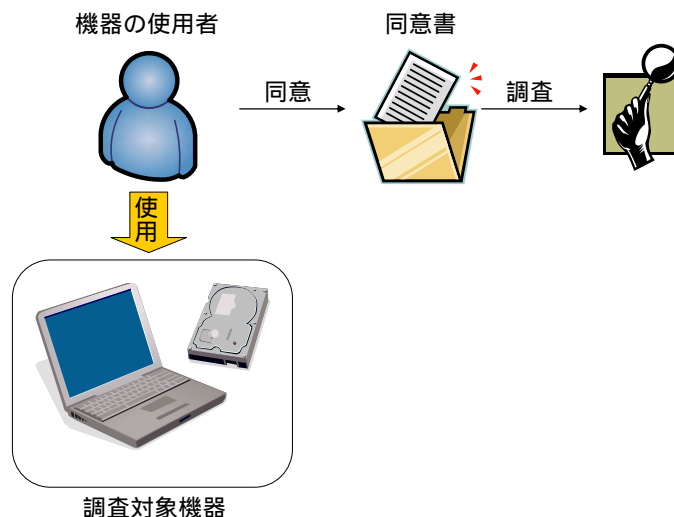


図 1

¹ ネットエージェントのフォレンジック調査サービスは調査対象機器に記録されているデジタル・データのみを調査対象としており、聞き込みなど「探偵業の業務の適正化に関する法律」に関連する探偵業務は、届出を行っていない関係上扱っておりません。

(3) ご依頼内容の確認

フォレンジック調査をご依頼いただく場合、まず「フォレンジック調査相談シート」をご記入いただき、簡単なヒアリングを実施させていただきます。本格的なフォレンジック調査を必要とするかをまずは確認したいといった場合には「プレビュー（閲覧）」サービスをご検討ください。「プレビュー（閲覧）」サービスの詳細につきましては弊社営業にお気軽にお問合せください。

お客様と秘密保持契約（NDA）を締結させていただいた後、「フォレンジック調査依頼書」にご記入をいただき、フォレンジック調査の目的・内容の詳細について弊社フォレンジック調査員との間でお打合せをさせていただきます。

お打合せの内容に従い、弊社フォレンジック調査員が実施する技術項目（調査項目）をリストアップさせていただき、お客様に実施内容をご確認いただきます。ご依頼いただく調査内容と、実施する項目により調査に必要となる期間・費用が変化いたします。

調査方針の決定

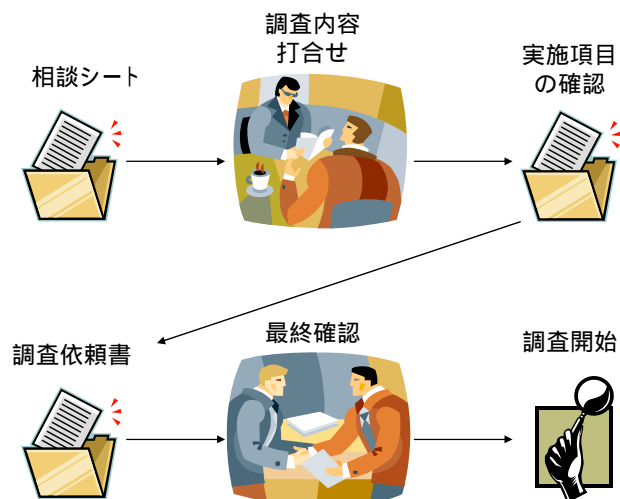


図 2

(4) 調査対象機器のデジタル・データの複製

ネットエージェントのフォレンジック調査では、調査対象機器(原本)²に保存されているデジタル・データを、専用装置または専用ソフトウェアを利用して一部または全てを複製いたします。

複製に利用する専用装置・ソフトウェアは、調査対象機器のデジタル・データを改変しないようにする機能(書込み禁止機能)を持っており、調査対象機器のデジタル・データを改変せずに複製することが可能となっております。

複製したデジタル・データは、調査対象機器のデジタル・データと同一であることをハッシュ値にて確認し、複製したデジタル・データをフォレンジック調査の対象といたします。³

複製の作成

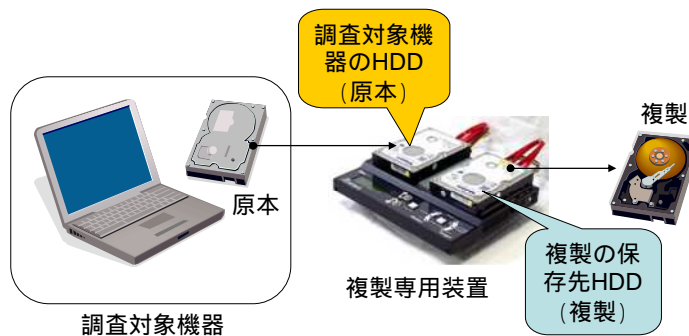


図 3

複製作業は、調査対象機器のデータ量(使用していない領域を含む)によって変化いたします。例えば、60GBのハードディスクをコピーするには、専用装置を使用した場合で約1時間の複製時間が必要となりますが、ハードディスクの回転数やセクタエラーの有無によっては、より長い時間が複製作業に必要となります。

さらに、原本と複製のデジタル・データが同一であることを確認するため、ハッシュ値を計算する

² 調査対象機器からハードディスクなどを取外す作業はお客様側での実施となります。

³ 調査対象機器に、読取りエラーが発生する箇所が存在する場合は、技術的に同一性の確認が実施できない場合があります。



作業に複製とほぼ同じ時間が必要となります。このため、60GB のハードディスクの複製と同一性の検証が完了するには最低でも 2 時間は必要となります。

複製専用装置を利用したデジタル・データの複製が技術的に困難な場合には、専用ソフトウェアによる複製を実施する必要があります。しかし、専用ソフトウェアによる複製は、専用装置を利用した場合よりも長い時間が必要となります。

専用ソフトウェアによる複製は、約 10GB / 時間と低速であり、60GB のハードディスクを複製するには約 6 時間の複製時間が必要となります。

RAID 装置のような機器に保存されているデジタル・データの一部(ファイル・パーティション・論理ドライブ単位)を複製するようなケースでは専用ソフトウェアによる複製を実施する必要があります。

(5) 調査の実施

お客様からのご依頼内容に従い、複製したデジタル・データに対して、弊社の調査員が専門的な調査を実施いたします。

フォレンジック調査で発見されたデジタル・データの結果確認・報告方針などの詳細につきましては、別紙「フォレンジック調査実施約款」をご参照ください。

また、お客様の業務に関連した「検索キーワード」などは、事前のお打合せ段階か調査開始後にご指定をいただき、解析専用ソフトウェア (EnCase) にてキーワードの検索・結果確認⁴などをさせていただきます。

削除ファイルや、削除されたファイルの断片・痕跡なども検索することができ、文字コードも複数の形式に対応したきめの細かい調査が可能になっております。(発見された文字列痕跡などに関する技術的なご説明などは、報告会にて詳細をご説明させていただく形を取っております)

調査の実施

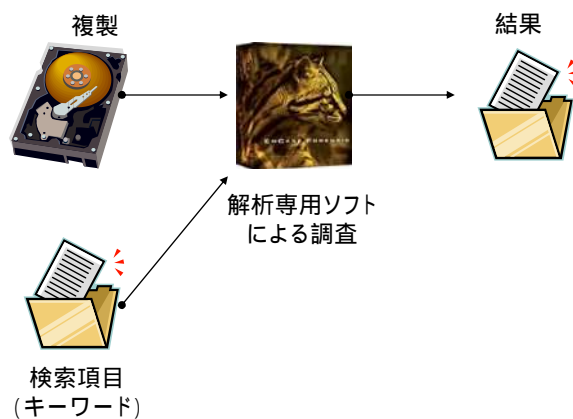


図 4

⁴ 検索結果につきましては、お客様にご確認いただける形 (CSV 形式) で提供させていただくことも可能です。

(6) 報告会

フォレンジック調査の結果につきましては、報告書と共に報告会を開催させていただきます。報告会は弊社調査員がお客様へお伺いする、または弊社にてご報告をさせていただきます。

報告会では、調査に使用した解析専用ソフトウェア(EnCase)の画面をプロジェクタで表示し、お客様に実際のデータをご覧いただきながら結果のご報告をさせていただきます。

報告書の記載内容で不明な点や、お客様の目で確認が必要な事項につきましては、その場で調査員が解析ソフトウェアを操作し疑問にお答えいたします。一般的な報告会では2~4時間程度のお時間が必要となります。

報告会

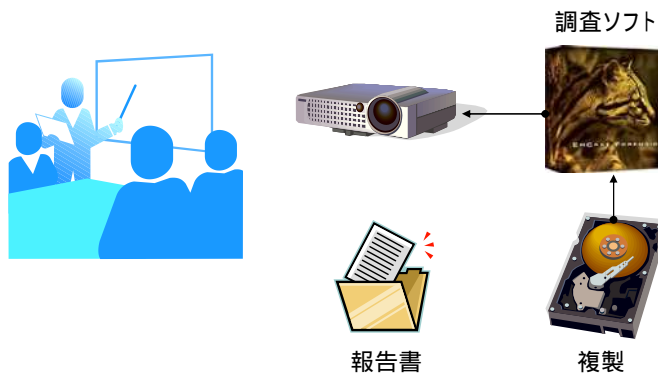


図 5

(7) 納品物

弊社からの納品物としては、通常以下をご提供しております。⁵

- ・ デジタルデータの写し作成及び同一性確認調査報告書
- ・ フォレンジック調査結果概要報告書
- ・ フォレンジック調査報告書(+記録ノート)
- ・ 複製ハードディスク(調査対象機器のデジタル・データを複製したもの)
- ・ その他(ファイルリストなど電子データを保存したメディア)

⁵ ご依頼の調査内容により、納品物は変化いたします



(8) 全体の流れ

1. インシデント発生
2. 調査端末の確保
3. ネットエージェントへの連絡
4. お客様へご訪問
5. 調査内容打ち合わせ
 1. > NDA(守秘義務契約書)確認
 2. > 相談シート確認
 3. > 実施項目確認
 4. > 調査依頼書確認
6. 最終確認後、調査スタート
7. 調査対象機器を確認
8. 複製作業へ
9. 解析専用ソフトウェアにて解析作業
10. 解析後、報告書作成作業
11. お客様へ報告会の実施

(9) お問い合わせ先

東京本社

〒130-0022

東京都墨田区江東橋 4-26-5 東京トラフィック錦糸町ビル 9 階

電話番号 03-5625-1245

FAX 番号 03-5625-9008

メール forensic@netagent.co.jp

ホームページ

<http://www.netagent.co.jp/>

<http://forensic.netagent.co.jp/>