Japan Forensic Instituteは、デジタル証拠保全・復元・調査・分析など、IT社会に潜む脅威から企業を保護し、支援するサービスを提供しています。

FORENSIC SOFTWARE & SERVICE

コンピュータフォレンジックで企業を守る。

Japan Forensic Institute FSS.jp

AOS フォレンジックのご紹介

AOSテクノロジーズ株式会社
〒105-0001 東京都港区虎ノ門5-1-5 虎ノ門45MT森ビル5F
URL: http://www.aos.com/

AOS　フォレンジックとは

　デジタルデータは、コピーしやすいだけでなく、原本とコピーの判別がしにくいという特徴があります。またデータを改ざんしたり、転送したり、削除することも容易に行えるために、「法的な証拠能力を有する」といえるためには、資料の収集、保管、分析、報告にいたるすべての過程において、特別な手続きと手法を踏まなくてはなりません。デジタルデータの法的な証拠能力を持つようにするための手続きを、「コンピュータ　フォレンジック」といいます。

デジタル データ

復元、収集、保管、
分析、報告

法的証拠

どうしてAOS　フォレンジックが必要なのか？

悪意のハッカーの攻撃によって情報漏洩などの被害を受けた場合、企業はどのように対処するべきでしょうか。特に情報サービスを提供する企業であれば、顧客情報が流出すれば企業イメージが大幅に低下するだけでなく、民事上・刑事上の責任を追求される可能性もあります。ハッカーが証拠を隠滅するために侵入した痕跡を消し去ってしまった場合、企業はどのようにして事実関係を究明し、法的な責任の範囲を明確にすればいいのでしょうか。それともセキュリティ管理の責任を超えて、実際に発生した被害すべてについて責任を負わなくてはならないのでしょうか。

AOS フォレンジックは、コンピュータをソフト的またはハード的に解体することによって得られるコンピュータ内に記憶されたデジタルの資料をもとに、証拠を収集し、事実関係を究明する手法です。 この手法は、民事・刑事上の事件の捜査だけでなく、通常の企業活動の中でも、従業員などの違法行為を発見したり、証拠を確保するために使われます。特に顧客との　紛争解決において、重要な証拠資料を保全するために必要となります。

Forensics　調査手順

1. ヒアリング：調査対象と内容の確認

まずフォレンジック調査の「依頼票」をご記入いただき、ヒアリングを実施します。
お客様の希望される調査項目をリストアップし、証拠調査の実施内容（作業方針）を確認します。

2. 調査媒体の保全

調査対象となる媒体（ハードディスクなど）を、専用機器で保全（全体を複製）します。
対象媒体のデータが改変されないようにする機能（書込み禁止機能）を持つ専用機器
で保全を行うことで、調査対象媒体のデジタル・データが改変されずに複製されます。
さらに複製したデータについて、オリジナル媒体のデータと同一であることをハッシュ値
で確認した後、複製したデジタルデータに対してフォレンジック調査を実施します。
このようにオリジナルデータを保全することで、非常に変質しやすく改変が容易なデジタ
ルデータに法的証拠能力が認められることとなります。

3. フォレンジック調査（解析）

コンピュータ・フォレンジック調査を実施し、有意な情報を抽出・解析します。
主に以下のようなデジタルデータを取得可能です。
・現存するファイル
・ゴミ箱から削除された（または断片化された）ファイルの検出
・故意に削除したファイル・インターネット閲覧履歴（WEBメールの痕跡、
WEBの閲覧履歴）
・パソコンに接続された外部ディスクの履歴

さらにご要望にあわせて詳細な情報を抽出することができます。大量のデータから必要かつ有意な情
を抽出し、そのコンピュータで何が行われていたのか浮かび上がらせる

・キーワードによる検索
（既に削除されたり断片化した過去のデータも含めて、キーワードや特定文字列によるファイルやメールの検索）
・特定期間中に作成・更新されたファイル ・ファイルの作成日時・更新日時・アクセス記録
（知財訴訟、データの改ざん疑惑など）
・インターネット閲覧履歴（通常の履歴には残っていない過去の情報も含む

4. 調査結果のご報告

調査結果をご報告いたします

事例1　Winnyによる情報漏えいファイル共有ソフト（Winny）による情報流出

内容：社員が、自宅で仕事をしようと会社のデータをUSBメモリに入れ、自宅のPCへ　コピーした。ところが自宅PCにはP2Pソフト（Winny）がインストールされており、暴露ウィルスにより業務ファイルがWinnyネットワーク上へ流出してしまった。

デジタル・フォレンジック調査結果

自宅PCに対してコンピュータフォレンジック調査を実施。その結果、Winnyインストールの履歴、暴露ウィルスの感染形跡、漏洩ファイルの特定・復元が可能になった。

さらにネットワーク上から漏えいファイルを収集し、PC内の業務データと一致することを確認した。

事例2　情報漏洩事件　外注先社員による不正アクセス

内容：大手企業の顧客リストに第三者から広告メール（DM）が発送され、
個人情報が漏えいしていることが明らかになった。

デジタル・フォレンジック調査結果

個人情報データベースを保存してあるサーバーにフォレンジック調査を実施し、不審なアクセスログを検出した。アクセス日時や権限情報などを分析し、顧客リスト管理の外注先社員が、インターネットカフェからServerに不正アクセスして個人情報を入手し、転売していたことが判明した。

事例3　窃盗団によるカーナビ被害　　データクリアされた盗品カーナビ

内容：窃盗団により盗まれたと思われるカーナビを確保したが、転売するためにカーナビの情報はクリアされていたため、盗品であることを証明する証拠データが必要となった。

デジタル・フォレンジック調査結果

フォレンジック調査を実施したところ、消去されたカーナビのデータを復元し、本来の所有者が保存したと思われる情報を確認できた。それによりカーナビが盗品であることが証明され、窃盗と転売に関係したグループの摘発につながった。

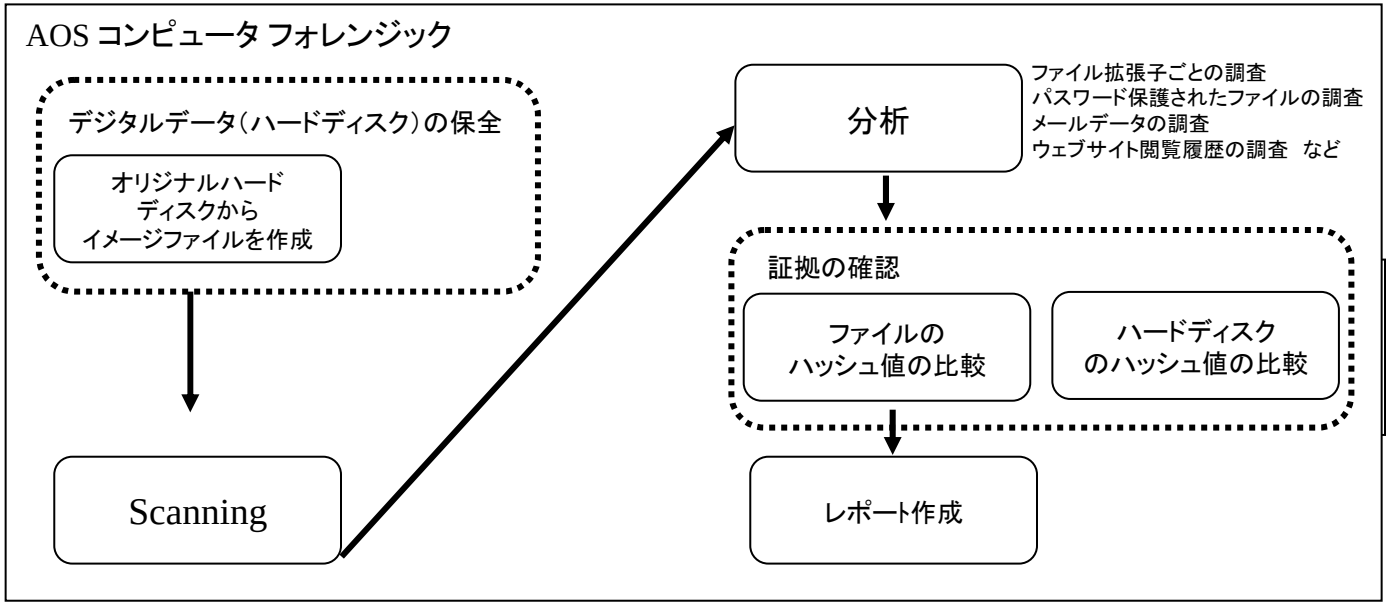
AOS フォレンジック の調査手順

1、AOS フォレンジック 証拠保全

2、AOS フォレンジック データリカバリー （消滅データの回復）

3、AOS フォレンジック データ解析及び復元

4、AOS フォレンジック 調査・報告



AOS フォレンジック データリカバリーの分析対象

a) 分析対象ファイルシステム

＊ Windowsのファイルシステム: FAT12/16/32、NTFS4.0/5.0/5.1

＊ Linuxのファイルシステム: EXT2、EXT3

＊ CD/DVDのファイルシステム: CDFS、 UDF

b) 分析対象メディア

ⅰ) HDD: 2.5インチと3.5インチのIDE/EIDE/SCSI/SATAインタフェースのハードドライブ

ⅱ) 光メディア: CD/CD-R/CD-RW、DVD/DVD-R/DVD+R

ⅲ) 携帯用記憶装置: FDD、USBメモリ、メモリカード(SD、CF、MS、MMC、xDなど)

ⅳ) 外部記憶装置: MO、ZIP、Jazドライブ

※ システム構成によっては、上に記載された分析対象メディアのいくつかはサポートすることができません。

AOS フォレンジックの機能・特徴

1. 様々なスキャン方法のサポート
   - 正常なファイルのスキャン、削除ファイルのスキャン、失われたファイルのスキャン
2. 検索結果の分類機能
   - 拡張子、時間（タイムライン分析）
3. 検索後のプレビューを素早く、多くの有用なS/Wをサポート
4. 日本語、現地で広く用いられているS/Wのサポート
5. 通常領域・削除データ領域のキーワード検索
6. 容易で簡便なGUI
7. 強力な削除ファイル復元
8. キャプチャなどの追加機能

AOS フォレンジックの証拠保全・分析機能

1. 正常なファイルの拡張子変造可否確認/分析機能
   => 正常なファイルの拡張子変造以前の拡張子検索
   及び検索結果表示機能 （証拠収集）

2. ハッシュ機能 ： MD5（SHA-1、SHA-2、SHA256など）
   => データの変造可否確認及び検証（証拠獲得）

3. 特殊検索機能 文字列やフォーマットで検索
   => 検索時検索オプション設定で特殊検索可能 （証拠分析/獲得）

4. 証拠調査レポートフォーム
   => 報告書作成機能

ＡＯＳ　フォレンジック事例　2008年度実績

Japan Forensic Instituteは、コンピュータの動作・アクセス履歴のようなログを取得し、一度消去されたデータを復元するといったデジタルフォレンジック技術によって、裁判などで有効な証拠性ある電子データを抽出します。
訴訟対応、内部監査、事件の捜査、医療事故調査、正当性の証明など、多様な目的に応じ、適切な証拠取得を支援いたします。

・労務管理訴訟 （過労死訴訟）
・情報漏洩 （競合他社への情報持ち出し）
・不正会計 （経営層による粉飾決算）
・機密情報の漏洩
・セクシュアル・ハラスメント （上司からのセクハラメール）
・Winnyによる情報漏えい
・窃盗団によるカーナビ被害 （盗品である証明）
・ウィルス被害 （感染原因・経路特定）
・情報漏洩 （外注先社員による不正アクセス）

基本的なデータ復元分析

ファイルやフォルダ単位のデータ復元

ごみ箱を空にするなど、単純に削除されたファイルやフォルダをツリー構造のままファイルやフォルダ単位で復元。

クラスタ検索

データ領域全体をスキャンして、ファイルフォーマット（拡張子）別に復元。

起動不可能な場合のデータ復元

MBRやFAT、MFT、I-nodeなどが損傷して起動できない場合にもデータ復元可能。
（システム復旧は不可）

フォーマット時のデータ復元

クイックフォーマットや通常フォーマットによって初期化されたドライブからのデータ復元。

ウィルスによって破損したデータ復元

CIH、WormExploreZip、LoveLetterウィルスなどによって損傷したデータを、クラスタ検索を通じて復元。

ボリューム破損後のデータ復元

パーティションやボリュームが破損して認識できない場合でも、該当のボリュームやパーティションを検索して復元。

クラッキングによる破損時のデータ復元

クラッキングによって起動できなくなったディスクからのデータ復元。

マルチファイルシステムのデータ復元

一つのハードディスクに FAT, NTFS など複数のファイルシステムを持つ場合にもデータ復元可能。

拡張データ復元分析

ネットワークデータ復元

TCP/IP、IPX/SPXプロトコルを使ったネットワークまたはインターネット経由のリモート復元機能。(ファイアウォールの場合にも該当ポートが開いていればリモート復元可能)

Officeファイル修復ウィザード

上書きによって破損または断片化したOfficeファイルに対して復元ウィザード機能を使ってデータを修復。

ディスク/ファイルビューアやプレビューアによるデータ分析/復元

復元の前にデータやディスクの内容を確認して分析することができ、ビューア内の検索を利用して、文字列や16進コードで探すことが可能。

ディスク/ファイルFATエディタによる破損したデータ復元

上書きによって一部破損したデータの場合、ビューアとディスク/ファイルFATエディタを利用して手動または自動的に復元。

カスタムファイルフォーマット検索によるデータ分析/復元

上書きよって破損または断片化したデータに対して、重要なデータの一部を復元する時や、特定ファイルの拡張子を持ったデータに対してデータ復元。

その他の機能

- 復元結果をレポートとして出力する機能。
- 一定のセクタ範囲を指定して保存機能でイメージを作成し精密分析に使用。