

## Ji2 ニュースレター (フォレンジック技術とE ディスカバリ)

2009年12月号

### はじめに

京都の清水寺で発表される毎年年末恒例の世相を表した今年の漢字は「新」であります。フォレンジック業界も訴訟支援技術業界の基礎テクノロジーとして重要な役割を担っておりますが、近年では電子文書業界との融合も始まり、まさしく「新」しい時代に突入しております。今米国では、電子文書管理業界の大手企業であるIBM、EMC、富士ゼロックスなどがフォレンジック業界や訴訟支援技術業界の企業を買収し新しいビジネスをスタートする動きもあります。

来年2月には米国NYにてLegal Techが開催され、弊社Ji2は展示参加いたします。そこで得られた業界動向や最「新」テクノロジーを次号のニュースレターで皆様にお届けしますのでご期待下さい。

### 内容

1. 最新ビジネス・ニュース.....	2
2. テクニカルニュース.....	4
3. イベント情報.....	6

\*弊社Ji2では、「法務部・知財部の情報開示 (E-Discovery) 対応簡易ガイド」をご希望の方に無料で送付させていただいております。本ガイドでは、eDiscovery対応手順の米国スタンダードを日本企業様向けに日本語で紹介しております。入手ご希望の方は弊社担当の保元(ヤスモト)までメールにてご連絡ください。E-Mail: [info@ji2.co.jp](mailto:info@ji2.co.jp)

**Note:** Ji2ニュースレターは、「フォレンジック」「インシデントレスポンス」「電子証拠開示 (eDiscovery) ディスカバリ」の分野で日米最新ニュースを「プロセス」と「技術」の2つにフォーカスしております。具体的にかバーするトピックは、リーガルテクノロジー (Legal Technology)、レビュープラットフォーム (Review Platform)、電子証拠開示技術 (eDiscovery)、米国裁判での事例紹介、フォレンジック最新技術です。日米発の最新情報を、いち早く日本語でお届けするニュースレターを2ヶ月に1度お届けして参ります。内容について、ご意見・ご要望などございましたら、ご遠慮なくお申し付けください。

**株式会社 Ji2:** 2001年より米国法人、そして2007年より日本法人を持つ日米ハイブリッド企業です。ディスカバリやフォレンジックのベスト・プラクティスと社内ソリューションをご提供致します。日米企業への豊富な経験をもとに、英語と日本語でディスカバリ作業や社内インフラ構築のコンサルティングのご提供が可能です。専門分野は、セキュリティ・コンプライアンス対応、コンピュータ・フォレンジック調査、訴訟対応に関連する「ソフトウェア販売」「ハードウェア販売」「トレーニング」「コンサルティング」で、特に米国訴訟における電子証拠開示 (eDiscovery) におきましては、迅速な日本語サポート体制とベストツールの活用により、顧客企業様に「サービス」と「プロセス構築」の両面からベスト・プラクティスをご提供致しております。 <http://www.ji2.co.jp>

## 1. 最新ビジネス・ニュース

---

### 米国訴訟で活躍するコンピュータ・フォレンジック技術

米国での刑事事件の科学調査は総称してフォレンジックと呼ばれます。その中で、コンピュータ・フォレンジック (computer forensic) / デジタル・フォレンジックとは、コンピュータや携帯電話などのデジタル・データに特化したフォレンジック技術で、消去された電子メールや画像、ウェブサイトの訪問履歴などを復元し、電子証拠データの改ざんがないことを証拠化することができる技術と理解されます。ただし、米国刑事・民事訴訟のディスカバリー時に、弁護士や検察官といった司法関係者はフォレンジックという言葉を用いて削除ファイルの復元技術という狭義で使いますので注意が必要です。

### マイケル・ジャクソンやタイガー・ウッズもコンピュータ・フォレンジック

2003年11月18日、サンタバーバラ郡シェリフは幼児虐待の容疑でマイケル・ジャクソンの自宅を家宅捜索し、70人を超える捜査員を動員してコンピュータやカメラに保存された画像やファイルなどを押収しました。このとき押収された電子メールや画像などの調査に使われたのがコンピュータ・フォレンジック技術です。この裁判は、全ての容疑に対してマイケル・ジャクソンの無罪が言い渡されるという形で幕を下ろしましたが、このときの調査はまさにコンピュータ・フォレンジック技術を駆使したものでした。また、ごく最近ではタイガー・ウッズの愛人問題で注目を浴びている電子メールですが、浮気調査などでは携帯電話の情報や、削除済み電子メールなどの復元にコンピュータ・フォレンジック技術が欠かせないものになっています。

### 訴訟で使えるフォレンジックツール

米国裁判において、消去されたデータや壊れたコンピュータ・携帯電話などの復元調査を「Order for FORENSIC search of party's computer system」や「Order for expedited FORENSIC imaging」などとして裁判所から要求されることがあります。一般的にフォレンジック作業は、特別な資格を持つフォレンジック調査官がフォレンジックツールを用いて行い、多くの時間を必要とするため高いコストが掛かります。よって、このコストを誰が負担し、フォレンジック調査によって得られる復元データが十分にそのコスト・時間に値するものであるかといったことが争点になります。

一般的に訴訟関連で使用されるフォレンジックツールは下記のような製品分野があります。

1. ハードディスク・イメージング (証拠取得・保全ツール)
2. 電子データ復元・解析ツール
3. メタデータ抽出ツール

フォレンジック製品と呼ばれるものは世界に数多く存在しますが、これらのツールは法廷で信頼性を問われるため、米国裁判において実績のあるものを選ぶことが大切です。実績のある有名なフォレンジックツールは、Encase, iLook, FTK, Paraben, X-Ways Forensics, SMART, Macintosh Forensic Software, Safelock, ProDiscover, Sleuthkit などがあります。他にも証拠取得・保全ツールはHDD複製装置などが多用され世界で約5社のメーカーが存在します。

### 知っていて便利な裁判技術用語

コンピュータ・フォレンジックでは、原本(保全証拠)とコピーの同一性を証明することが鉄則です。電子データの同一性の確認は下記の技術が中心となります。

**ハッシュ値 [Hash Value]**: 文書やメールなどの電子データを、一定長のデータに要約するための関数をハッシュ関数という。関数を通して出力される値は、「ハッシュ値」、または単に「ハッシュ」と呼ぶ。法廷で用いられる代表的なハッシュ関数は“MD5”で、原本とコピーが同じハッシュ値であれば、同一性が証明される。

**メタデータ [metadata]**: 電子データについてのデータ。コンピュータのファイルなどについて、そのデータの作成者、作成日時、属性などを記録したもので通常は隠れて見えない情報。この情報が証言や本文の情報と一致することで証拠の連続性が確認できる。

#### これからの訴訟にフォレンジック技術がもたらす変化

近年、米国裁判において電子メールや電子文書が証拠となるケースが増加しています。この電子文書に対して、証拠性を証明するのがコンピュータ・フォレンジック技術です。近年のフォレンジック技術では携帯電話やコンピュータ上の電子メールや画像、ウェブサイトの履歴などを消去しても復元可能であると仮定して裁判に望むことが大切です。つまり、安易に電子データを消去、隠ぺい、改ざんすることが、逆に不利となることを理解し、存在する不利・有利なデータを把握した上で、提出・不提出などの戦略を弁護士事務所と相談することをお勧めします。

## 2. テクニカルニュース

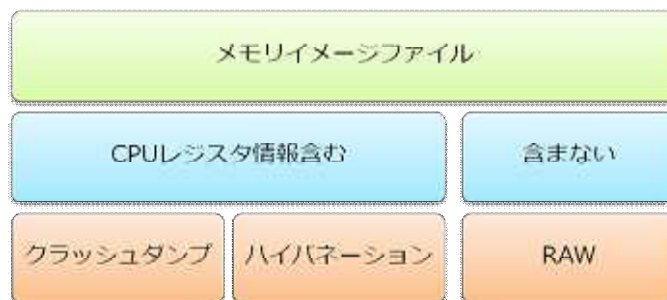
### メモリエージ解析 ちょっといい話 Vol.2「どんなツールがありますか？」

#### 1. メモリエージの種類

メモリエージにはいくつか種類があり、CPUレジスタの情報を含むクラッシュダンプファイルやハイバネーションファイル、レジスタの情報を含まないRAW イメージがあります。

メモリフォレンジクスという一般にはRAW イメージの解析が中心ですが、とくに問題なければレジスタ情報も収集できるとベストです。最近では Windd と呼ばれるツールがクラッシュダンプファイルの取得に対応しています。

RAW イメージを解析するツールは様々ありますが、クラッシュダンプファイルを解析するツールは、現在のところ Microsoft が提供している WinDbg と呼ばれるカーネルデバッグツールしかありません。WinDbg は全ての WindowsOS に対応していますが、そのままでは情報の取得や文字列の検索に難があります(スクリプトを使えばある程度は拡張可能)。以降は RAW イメージの取得ツール、解析ツールをご紹介します。



#### 2. メモリエージの取得ツール

RAW イメージ取得ツールには ManTech Memory DD, Windd, FastDump Pro などがあります。ManTech Memory DD を除いて他はソースコードがクローズドなため、どのような実装になっているかは正確には分かりませんが、ツールによっては 4GB 以上のメモリエージ取得に対応できない、物理メモリの最初の 1 フレーム (4kB) を取得できないなどの問題があります。これにより、例えば Volatility Framework のような解析ツールがイメージを解析できない、という事象が発生します(詳しくは以下の記事をご参考ください)。

<http://cci.cocolog-nifty.com/blog/2009/06/pfn-0.html>

#### 3. メモリエージの解析ツール

解析ツールの実装手法は主に以下の二通りに分類されます。

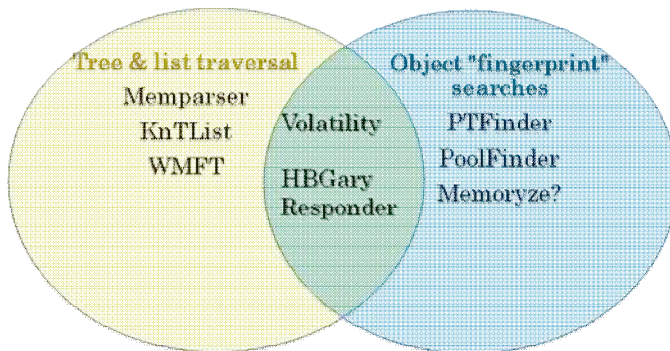
- ✓ Tree & list traversal

OS のメモリ管理オペレーションを再現します。具体的には、仮想アドレスの変換を行い、取得したアドレスから Windows カーネルのデータ構造体 (\_EPROCESS など) にアクセスして必要な情報を取得します。

- ✓ Object “fingerprint” searches

仮想アドレスの変換は行わず、メモリエージ内のカーネルデータのシグネチャを網羅的に検索します。

以下に解析ツールの実装手法ごとのツールの分類を示します。Volatility FrameworkとHBGary Responderは2つの手法の両方を実装しています。



次に手法別のメリット&デメリットを示します。

Tree & list traversal は仮想アドレスの変換をしながらプロセス構造体(EPROCESS)やモジュール構造体(LDR\_MODULE)のリンクリストをアクセスしていきます。リンクリストの先頭(プロセスであればPsActiveProcessHead、モジュールであればPsLoadedModuleList)を取得した後は芋づる式にデータを取得できるため、処理にかかる時間は少なく、ノイズもありません。しかし、解析の過程で利用するデータを含むメモリページが何らかの理由で取得できないor壊れている場合は、全てのデータが取得できなくなります。加えてDKOM(Direct Kernel Object Manipulation)のような、ルートキットが用いる隠蔽のテクニックに対して耐性がありません。

一方で、Object "fingerprint" searches は不完全なメモリイメージでも情報を取得できたり、DKOMのような攻撃を検出できる反面、網羅的な検索を行うため処理にかかる時間が増え、ノイズデータを出力する可能性もあります。



ツールを使う側としては、このような使用するツールごとの特性を理解したうえで利用する必要があります。

### 3. イベント情報

---

#### 日本国内

- ・EnCase Computer Forensic トレーニング **受付中(受付締切 1/29)**  
日時: 2010年3月1日 ~ 4日 9時 ~ 18時  
場所: 株式会社Ji2 セミナールーム
- ・クイックリファレンスコース(eMail) **受付中(受付締切 1/29)**  
日時: 2010年3月5日(金) 13時 ~ 18時 (5時間)  
場所: 株式会社Ji2 セミナールーム
- ・EnCase Computer Forensic トレーニング **受付中(受付締切 1/29)**  
日時: 2010年3月8日 ~ 11日 9時 ~ 18時  
場所: 株式会社Ji2 セミナールーム
- ・Windowsフォレンジックのための要素技術セミナー **受付中(受付締切 2/26)**  
日時: 2010年3月15日 ~ 16日 9時 ~ 18時  
場所: 株式会社Ji2 セミナールーム

トレーニングのお申込みにつきましては下記URL先をご参照ください。  
<http://www.ji2.co.jp/training/>

#### 米国

- ・LegalTech in New York出展 **New**  
日時: 2010年2月1日 ~ 3日  
場所: The Hilton New York Hotel  
<http://www.legaltechshow.com/>

---

ニュースレターの登録、解除等については、下記連絡先までご連絡ください。  
本ニュースレターに関するご要望、ご意見をお待ちしております。

編集・発行

株式会社 Ji2 (発行担当: 佐藤)

E-mail: [newsletter@ji2.co.jp](mailto:newsletter@ji2.co.jp)

米国事務所: 11235 Knott Ave. Suite C. Cypress, CA 90630 U.S.A.

日本事務所: 〒160-0004 〒160-0022 東京都新宿区新宿 1-9-5 大台ビル 3F

TEL: 03-6228-0163 FAX: 03-6228-0164 <http://www.ji2.co.jp/>

---