

## 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)

2010年8月号

### はじめに

米国でのトヨタ自動車の大量リコール（回収・無償修理）問題を巡り、米ウォールストリート・ジャーナルは、「米運輸省がトヨタに有利な情報を隠蔽していた。」というショッキングな記事を掲載しました。同省の高速道路交通安全局（NHTSA）で、当時リコール担当のチーフを務めていたジョージ・パーソン氏によると、「車が急加速したため事故を起こした。」と訴えがあった複数のトヨタ車について調査し、いずれも「運転ミスによる可能性が高い。」とのデータが集まりました。しかし「幹部らがデータを公表しないよう決定した。」とのことです。

パーソン氏はこれについて「データを公表すると、NHTSAはトヨタを擁護していると取られ、批判されることを恐れた。トヨタ問題に対する世間の関心は非常に大きく、政治的に事実など言えるわけがなかった」との見方を示しました。

真相はこれから明らかにされていくと思われませんが、少なくともこうした恣意的な判断に日本企業が巻き込まれることがあります。トヨタ自動車はこのために、膨大なディスカバリを実施する結果となりました。日本企業はこれらのバッシングの中でも、コンプライアンス遵守した誠実な対応をするしかない、改めて考えさせられるニュースでした。

### 目次

1. 最新ビジネス・ニュース.....	2
2. フォレンジック調査チーム便り.....	4
3. イベント・トレーニング情報.....	8

Ji2では、「法務部・知財部の情報開示（Eディスカバリ）対応簡易ガイド」や「Sedona Conference（業界標準規格）を元に社内教育用のディスカバリーセミナーを無料で開催させていております。社内教育セミナーをご希望の方は弊社保元(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)

株式会社Ji2は、2001年より米国法人、そして2007年より日本法人が設立され、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ております。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が可能です。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最善の方法をご提案致します。 <http://www.ji2.co.jp>

Ji2ニュースレターは、「フォレンジック」「電子証拠開示（eDiscovery）ディスカバリ」関連の日米最新情報を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お申し付けください。

## 1. 最新ビジネス・ニュース

---

### 日本企業の社内データ保全問題

日本企業を対象とした、米国訴訟における E ディスカバリ要求は年々増加していますが、弊社 Ji2 の仕事柄、証拠保全時直前の**故意的な削除メール**をよく目にします。これは特に社内 IT 部門が実施した E ディスカバリ時の保全データからよく見つかります。

最近の例では、ある日本大手企業が自主的に証拠保全したデータを相手方に提出しました。その電子メールの中から削除行為の痕跡があり、弊社が消去データ復元を担当し 3,000 通くらいの日本語メールが復元され、相手側に再提出しています。

ここでも問題点は幾つかありますが、日本企業に遵守して欲しいのは「事前に電子メールなどを消さない」「社内データ保全は法廷で説明可能なプロセスとツールを使用」「証言録取を準備」などです。

今回のある日本大手企業では消去データを巡り、社内自主データ保全した全員の証言録取を相手側から要求され、また裁判上不利な状況、費用的にも負担大という結果になってしまいました。

### 受け取った後に消滅する E メール

#### <一瞬のちに消滅する E メール>

消去メールにちなんだ対応ですが、最初から Eメールの保管を止めてしまおうというこのソフトウェア、その名も VaporStream (<https://www.vaporstream.com/>) 送受信したメールが跡形もなく消えるソフトウェアが話題を集めています。

#### <消える Eメールの仕組み>

このメールソフトを使うと、送信メールが瞬時にして送信者の PC やスマートフォンから消去されます。同様に、受信側でも既読あるいは返信後に同メールは消去されます。さらに、メールの印刷や転送、あるいは添付ファイルの保存もブロックしてくれるのです。送受信者双方にインストールする必要がありますが、Outlook や Lotus Notes に統合することができ、PC だけでなく iPhone や Blackberry で使用することもできます。

このソフトウェアを使用した Eメール送受信の仕組みはこうなっています。

- 送信：送信側に記録は一切残らず → ベンダーサーバ → 受信：クリックして開いた時点でサーバから消去
- 添付ファイル送信 → ベンダーサーバ上でネイティブファイルからイメージファイルに変換 → 受信：保存できない形式で表示

Eメールのヘッダーとボディを分けて送信するため、万が一画面をキャプチャしても、内容と送受信者を結びつけることはできないとされています。また、ベンダーのサーバではメッセージは RAM にのみ保管されるため、記録が残ることはないのだそうです。この他にも、キーワードフィルタリングという機能を利用して、設定したキーワードを含む会話の発生自体をブロックすることができます。リーマン・ブラザーズ破綻の調査では、「serious trouble」、「don't

share this」などのキーワードを基に見つかった同社のEメールが開示され、改めてEメールのリスクが浮き彫りになりました。

#### <データスリム化への一歩>

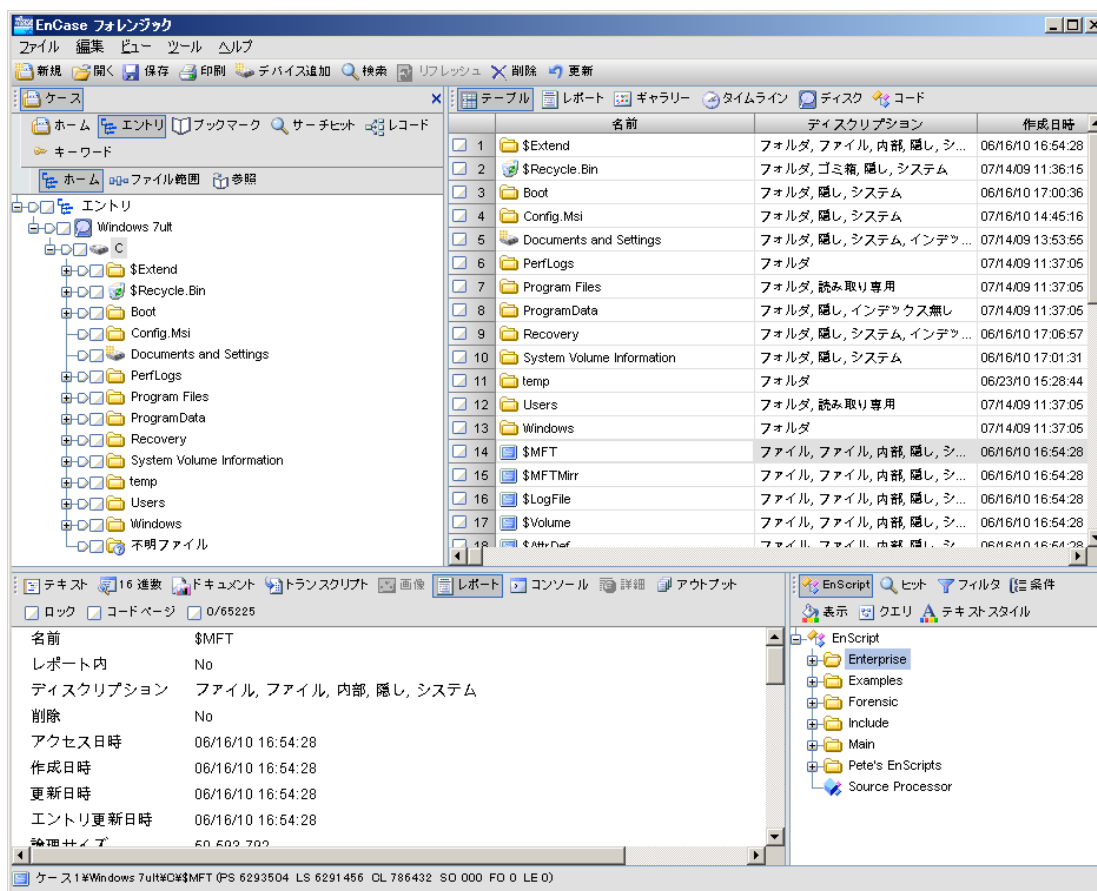
データや記録の保存に関するコンプライアンスという観点から、企業での全てのコミュニケーションをこうした形で行うことは不可能です。しかし、法的・業務的に必要のないデータまで保存しては、ストレージコストはかさむばかりです。さらに、要らない物が増えれば、要る物を探す時間もコストも増大します。消えるEメールが今すぐ広く採用されるのは難しいでしょう。しかし、このようなテクノロジーの出現は、リスクの再確認と、何もかも保存するというマインドセットを切り替える良いきっかけとなるのではないのでしょうか。

## 2. フォレンジック調査チーム便り

### 1. EnCase 日本語版の GUI が大幅に改善されました

EnCase 最新版バージョンの 6.17 では、日本語版 GUI の単語が修正・改善されています。これまでの日本語版 GUI では、訳語が適切でない箇所や、十分に日本語化されていない部分がありましたが、EnCase Ver 6.17 日本語版では大幅な見直しが行なわれています。若干、まだ違和感を覚える箇所もあるとは思いますが、ぜひご利用いただければ幸いです。何かお気づきの点などありましたら、お気軽に弊社までご意見いただければ、今後の改善に参考にさせていただきます。

(EnScript モジュールは日本語化されておりません。)



また、今後の EnCase トレーニング (CF1, CF2) においても、日本語版 EnCase を利用する予定となっており、トレーニング受講者の方に EnCase を理解いただく上で、日本語版は大きな助けになると考えております。

日本語版を含む最新バージョンの入手方法ですが、下記ガイダンスソフトウェア社のレジストレーションページから、ダングル (セキュリティキー) 番号を指定いただくことで、ダウンロード URL が記載されたメールが、ご指定のメールアドレス宛てに送付されます。

EnCase v6 Product Registration

<http://www.guidancesoftware.com/myaccount/registration.aspx>

※Japanese のチェックボックスを選択いただくと、日本語版の URL が含まれます

## 2. HBgary 社から無償の FGET ツールが公開されています

商用のメモリ・フォレンジックツール Responder を提供している HBgary 社から、ロックされているファイルなどのフォレンジックコピーを可能とする、“Forensic Get”、略して FGET ツールが公開されています。

FGET v1.0 Goes Live!!

<http://www.hbgary.com/community/shawnblog/fget-v10-goes-live/>

このツールは、ネットワークを経由して指定したターゲットコンピュータから、ファイルをコピーすることが出来るツールです。任意のファイルを個別に指定してコピーすることも出来ますが、対象ファイルを指定しない場合には以下のデータが自動的に収集されます。

- ・各ユーザーの NTUSER.DAT ファイル
- ・Prefetch フォルダ内のプリフェッチファイル
- ・windows¥system32¥config フォルダ内のファイル（レジストリ、イベント類）

FGET の特徴として、使用中やロックされているファイル、通常ではアクセスできないファイルについてもコピー元として指定することができます。例えば、Pagefile.sys や \$MFT といったファイルは、エクスプローラーを利用してコピーすることはできませんが、FGET では -extract オプションを指定することで、これらのファイルをコピーすることが可能です。例えば、削除されたファイルが NTFS レコード内に存在している場合、\$MFT をコピーすることでそれら削除ファイルを含む形で \$MFT ファイルを入手できます。（\$MFT ファイルをパースするには別途ツール等が必要になります。FGET で削除ファイルを取り出せるわけではない点に注意してください。）

FGET が自動的に収集したファイルは、プログラムを実行したコンピュータの C:¥FGETREPOSITORY¥フォルダ配下に、コンピュータ名でフォルダが作成され、HPAK 形式でデータが保存されます。HPAK ファイル内にあるファイルは、FGET ツールを使って取り出すことが可能です。（HPAK は HBgary 社が利用している専用のファイル形式です。）

ネットワーク上にあるコンピュータからデータを収集するには、ターゲットとなる Windows コンピュータで 135/tcp と 139/tcp ポートの通信が許可されている必要があります。FGET ツールを実行すると、ターゲットコンピュータ上で有効な認証情報を求めるダイアログが表示されるので、そこでユーザー名とパスワードを入力します。認証が完了すると、対象コンピュータからデータの収集やファイルのコピーが行なわれます。なお、Windows FireWall などでパケットがフィルタされている場合には、何も収集が行なわれず FGET が終了します。

ローカル上での実行も可能ですので、例えば使用中ファイルやロックされているファイルをコピーしたいといったケースでも FGET を利用することでファイルのコピーが可能になります。

F-ResponseとEnCaseを組み合わせるなどの方法を取れば、同様の作業が可能ですが、専用ツールが無い場合でも、簡単に特殊ファイルをコピーできるという点は、非常に便利ではないでしょうか。

**3. EnCase® Enterprise および Forensicの最新版 ver. 6.17が公開されました。**

Version 6.17では以下の拡張が行われています。

**(a) Windows Rights Management Services (RMS)**

Microsoft Outlook email や Microsoft Office の RMS が適用されたドキュメントの復号化ができるようになりました。

対応製品は下記の通りです。

- Office 2003、2007
- Outlook 2003、2007 PST

※この機能を活用するためにはEnCase Decryption Suiteが必要となります。

**(b) VMware 6.5&7**

VMware 上での動作に対応しました。例) EnCase Examiner と SAFE は下記製品の環境で使用可能になりました：

- VMware Workstation 6.5
- VMware Workstation 7.0
- VMware Server 1.1 (GSX)
- VMware vSphere 4.0 ESXi

**(c) Boot Camp 10.5 & 10.6**

EnCase Examiner と SAFE が Boot Camp 10.5 と 10.6 に対応致しました。

- Boot Camp v2.0
- Boot Camp v3.0

**(d) Guardian Edge Hard Disk と Symantec Endpoint Encryption**

GuardianEdge Hard Disk (GEHD) の下記バージョンと、Symantec Endpoint Encryption (SEE) データの復元が可能になりました。

- GEHD 9.2.2 and SEE 7.0.2
- GEHD 9.3.0 and SEE 7.0.3

※この機能を活用するためにはEnCase Decryption Suiteが必要となります。

**(e) 4KB セクタの HDD サポート**

Windows Vista や Windows 7 環境で使われている 4KB セクタの HDD を認識・解析が可能になりました。

**(f) Windows 7 の UDF 構造の解析**

Windows 7 で使われている UDF 構造 (バージョン 2.01 まで) の解析が可能になりました。

**4. EnCase® Enterprise ver. 6.17のみの新機能**

**(a) MAC OS X 10.6 Servret Support**

OS X 10.6にサブレットを配布/展開することが可能になりました。

**5. EnCase® Portable 2.2の新機能◆**

**(a) Personally Identifiable Information (PII) Triage**

個人情報検知モジュール(PII) Triageが搭載されたことにより、データを収集する前に、収集対象のマシンが危険な個人情報をもっているか否かを知ることができるようになりました。PII Triageを実行することで、ユーザーは以下の様な情報を含むファイル存在を、リアルタイムで知ることができます。

- クレジットカード
- 電話番号
- メールアドレス
- ソーシャルセキュリティナンバー

**(b) Capture Machine Information for Collection Jobs**

収集時にターゲットマシンの以下の様な情報を収集することが可能になりました。

- 対象マシン情報のサマリー
- ネットワークインターフェース
- ネットワークユーザー
- ネットワークルーティングテーブル
- ARP テーブル

**(c) Adding Machine Information to Reports**

収集時にターゲットマシンの以下の様な情報を収集するターゲットリストテーブル内のマシンの解析作業をする際、レポートにマシンの重要な基本情報を入力することが可能になりました。必須の証拠情報をマニュアルで入力する必要がなくなりました。

**(d) Include Images in Reports**

発見された情報の容易に共有できるように、画像をレポートに入れることが可能になりました。画像のサムネイルを含むレポートを、収集されたファイルから直ちに出力できるようになりました。

**(e) New Windows PE Operating System & CodeMeter Versions**

EnCase Portableは様々なハードウェアの起動をサポートしているWindows PE 3.0を現在使用しています。また、Code Meter セキュリティキーをサポートしているソフトウェアがアップデートされました。

### 3. イベント・トレーニング情報

---

#### その他日本国内のトレーニング

- **Windowsフォレンジックのための要素技術セミナー (受付中)**  
日時： 2010年11月24日～25日 9時～18時  
場所：株式会社Ji2 セミナールーム  
<http://www.ji2.co.jp/seminar/security/schedule.html>
  
- **EnCase Computer Forensic I トレーニング (受付中)**  
日時： 2010年11月30日～12月3日 9時～18時  
場所：株式会社Ji2 セミナールーム
  
- **EnCase Computer Forensic II トレーニング (受付中)**  
日時： 2010年12月7日～10日 9時～18時  
場所：株式会社Ji2 セミナールーム
  
- **EnCase Computer Forensic I トレーニング**  
日時： 2011年2月28日～3月3日 9時～18時  
場所：株式会社Ji2 セミナールーム
  
- **EnCase Computer Forensic II トレーニング**  
日時： 2011年3月7日～11日 9時～18時  
場所：株式会社Ji2 セミナールーム

---

■ 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：佐藤俊夫)

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：〒160-0022 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/>

---