

Ji2 ニュースレター (フォレンジック / eDiscovery)

2009年8月号

はじめに

米国の8月29日(金)に「Toyota Accused of Hiding Evidence」というニュースがメディアで一斉に流れました。この訴訟は、2003年から2007年までトヨタ自動車の社内弁護士であったDimitrios P. Biller氏が彼の携わったトヨタのSUVなどのPL(製造物責任)訴訟で、「トヨタは不利になる電子証拠を隠蔽した」という内容です。http://www.cbsnews.com/stories/2009/08/29/cbsnews_investigates/main5273636.shtml 真相はこれから裁判で明確となってくるとは思いますが、このニュースは日本企業の訴訟に下記2点で大きな影響を与えられと考えられます。

1. 米国裁判での日本企業における電子証拠開示に対する疑問視化(この事件で、日本企業への電子証拠開示(eDiscovery)体制の信頼性が疑問視され、これからの日本企業関連案件で隠蔽体制を確認される。)
2. 日本企業の社内弁護士でさえ、内部証拠開示の不備を指摘され訴訟になる可能性への対応

このニュースの直後に、いくつかの弁護士事務所のパートナーの方が、日本企業の社内証拠手開示体制を懸念されていました。今後は日本企業が巻き込まれる米国訴訟で、これまで以上に証拠開示が争点になると予想されます。

目次

1. 最新ビジネスのニュース	3
2. テクニカルニュース	5
3. 製品・サービス紹介(Legal Tech 展示会にて)	5
4. アップデート情報	11
5. イベント情報	8

*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

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)」の各ビジネス分野の日米のパイオニアとして最新ニュースを「ビジネス」と「技術」の2つにフォーカスして発信しております。今後カバーするトピック・キーワードと致しましては、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などを予定しております。日米発のフォレンジック、インシデント・レスポンス情報を、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。eDiscovery 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、英語と日本語でフォレンジックや eDiscovery 作業やその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。事業分野は、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「コスト」と「効率」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。 www.ji2.co.jp

1. 最新ビジネス・ニュース

日本企業が巻き込まれた特許侵害の訴訟ケースから学ぶ

米国訴訟対応時における日系企業での注意点

企業が保管する電子文書と情報量の膨大化により、近年の米国訴訟費用は特許訴訟では1件あたり平均4億円以上、最低でも5,000万円以上となっています。*AIPLA Survey
日系企業をとりまく訴訟は、2006年12月の連邦民事訴訟規則(FRCP)の改正**と、中国・韓国を始めとするアジア諸国の日系企業ターゲット化により、今後更に増えると予測されます。こうした訴訟への対応、中でも米国発端の電子証拠開示手続き(eDiscovery)への対応は、日系企業の社内文書管理体制に大きな変化を要求しています。

アダムス 対 デルの特許侵害訴訟 (Adams vs. Dell, 2009, Utah)

Dell、富士通、ソニー、ASUSなど十数社がフロッピーディスクに関する特許侵害で訴えられた訴訟。被告のASUS社による証拠電子メールの破棄の適切性が争点となった。

**本ケースの詳細な内容は www.ji2.co.jp/ediscoveryblog まで、法的な解釈は専門法律事務所までお問い合わせください。

本件で問題となったのは、下記の2点におけるASUS社の電子文書管理体制でした。

1. 社内文書管理規定に従う電子文書の破棄: ASUS社は社内文書管理規定により電子文書保存期間を定めていたが、管理が徹底しておらず、個人に電子メールの破棄を行わせるなど電子文書破棄の実行に一貫性がなかった。

2. 訴訟ホールドの開始時期: ASUS社の法務部・知財部は、原告の弁護士から特許侵害に関する書面を受け取った2005年2月が訴訟ホールド***の開始時期と理解した。それに対し裁判所は、類似する一連の大規模な訴訟が(Dell、富士通、ソニーなどへ)1999~2000年に発生しており、ASUS社はこの時点で訴訟を合理的に予測することが出来たと判断し、1999年時点から通常の電子メールの破棄を停止し、保全を開始すべきであったとした。

***訴訟時のデータ保存のプロセスを訴訟ホールド(litigation hold)と呼び、社内の保存ポリシーに則った通常サイクルでのデータ破棄を停止し、関連社員への通達も含めログを保管する必要があります。

日系企業での新しい電子文書管理のチェック項目

アダムス対デルの特許侵害訴訟などの例は、近年電子文書や電子メールの管理体制が企業側に問われていることを浮き彫りにしています。このような傾向に伴い、社内文書管理の不備によるSpoliation(証拠の破棄)と裁判所が判断し、制裁金を課すケースも増えています。今一度、社内の電子文書管理システムを下記の観点から見直してみてください。

- 法務部や知財部は、同業他社の類似訴訟から、直接自社に訴訟が発生していなくても、自社への訴訟の可能性を予測する。その予測される訴訟関連の電子メールを含む文書は全て訴訟ホールドの手順に従って保全する。
- 電子メールなどの破棄は、社内ポリシーに従い、システム化された一貫性のある運用を行う。
- 電子メールは、訴訟のリスクという観点から重要な公的文書と定義し、会社の実印が押されている正式文書と同等に扱う。さらに、書き方・運用において社員を徹底的に教育する。特に電子メールでの下記のような行為は厳禁とする。
ジョーク、不適切な表現、ネガティブな内容

会社や社員に不利となるコメント
違法性や不適切性のある事柄へのコメント
会社や社員に対する意見
会社と違う考え方の議論など

- 品質保証部などの製品検査結果の報告書やメールでは、個人的な見解や結果に対するコメントは不要。必要な場合は正式報告書に記載する。メモやメール内の個人的なコメントとして報告書と違う内容は一切残さない。
- 会議のメモを取る日本人は多いが、そのメモがよく訴訟の開示対象となる。よって、全体の決議や議論の内容に反する個人的な意見や、決定事項に反対する考え方などはメモで残さない。どうしても必要な場合は、個人的なメモではなく議事録などにする。

社内文書管理ポリシーのパラダイムシフト

電子メールを含め、紙媒体に代わる電子文書の過去 10 年間の爆発的な普及は、企業の社内文書管理に大きなパラダイムシフトを起こしました。大量の情報を含む電子文書は IT 部門がシステム導入し、文書管理部門が整理整頓・カテゴリー化を行いました。こうしてシステム化したデータを経理部や人事部が活用し、仕事の効率を向上させまし、技術部は図面や設計情報の電子化により情報の共有化(ナレッジ・マネージメント)に成功しました。もちろん、電子メールで社内外のコミュニケーションを行うシステムも利用できるようになりました。

今、このパラダイムシフトの中で、知財部・法務部が訴訟に備えてこうした電子システムの中から証拠開示に対応する必要が出ております。95%以上が和解すると言われる米国訴訟においては、いかに有利な和解条件を引き出すかが訴訟当事者双方の争点になり、相手方の電子証拠開示 (eDiscovery) プロセスを困難にする--相手方の保全対象データをなるべく増やし、かつ短期間で処理を行なわせる--という戦略も見られます。このような相手方の要求に応えるのは知財部・法務部の役割です。知財部・法務部の方は、社内電子文書管理の見直しを行い、もう一度自社の訴訟に対する備えを確認してみてください。

オラクルは EnCase eDiscovery を選択しました

ガイダンスソフトウェア社 (GSI) は、世界最大のビジネスソフト会社であるオラクルが GSI の EnCase eDiscovery を選択したと発表しました。

GSI の社長兼 CEO の Victor Limongelli は、「オラクルのような企業規模の会社が顧客名簿に載ったことを歓迎する」と述べました。「EnCase eDiscovery と共に、Oracle は eDiscovery コストを最小リスクで達成するのを待っています。」

「GSI は我々の法的要求に強い理解を示すことで名を上げました。」とオラクルの Pallab Chakraborty eDiscovery 担当取締役は述べました。「我々は eDiscovery プロセスを合理化、単純化してくれるこの強力な社内解決ソリューションを選択しました。」

EnCase eDiscovery は、電子的に格納された情報 (ESI) の検索、コレクション、保全とプロセッシングの主要な eDiscovery ソリューションです。それは、構造化されていない、もしくは半体系化されただけのデータとして置かれている ESI に対して、ビジネスの混乱を起こさずに、デスクトップ、ラップトップ、ファイルサーバ、電子メールサーバ、内容管理システムとリムーバブルメディア等のデータに対して、自動検索、コレクションや保全を行います。さらに、オプションでリティゲーションホールドや追跡機能も提供できます。その大きな処理能力は事前選別や細分化を可能にするだけでなく、メジャーな弁護士向けレビュープラットフォームのためのデータセットを作成し、顧客が大幅に処理経費を下げるのに役立ちます。

GSI は、Socha-Gelbmann の 2008 年度 e ディスカバリー部門の eDiscovery Software Providers Category で最も高いトップ 5 プロバイダに選ばれています。

2. テクニカルニュース

EnCase EnScript 作成入門 その2

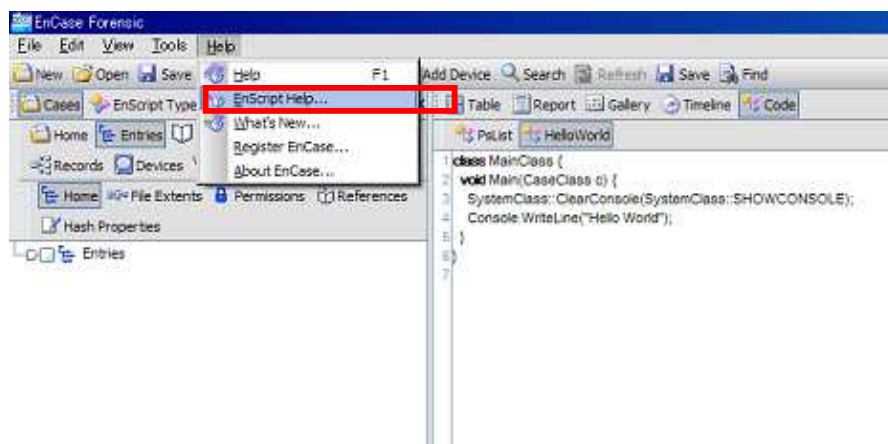
今回は、Hello World をコンソールに出力する最初の EnScript を作りました。

```
class MainClass {
    void Main(CaseClass c) {
        Console.WriteLine("Hello World");
    }
}
```

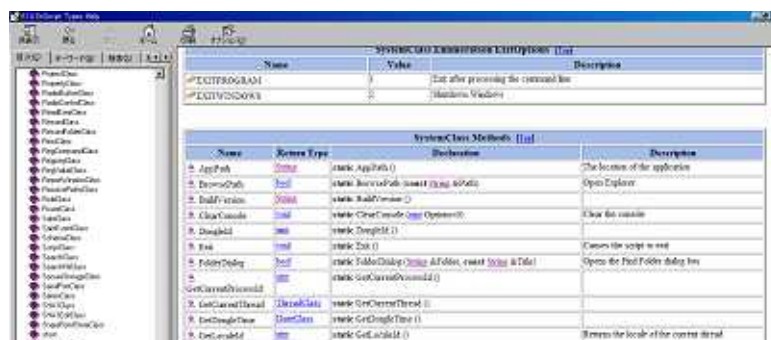
以下の命令を加えることで、コンソールの出力内容が実行の度にクリアされるようになります。

```
SystemClass::ClearConsole(SystemClass::SHOWCONSOLE);
```

この命令が何を行っているか？を調べるには、2つの方法があります。1つはメニューから EnScript のヘルプを起動して該当するクラスを調べることです。



ヘルプの目次で「SystemClass」を選ぶと、その中に ClearConsole メソッドがあります。説明によるとコンソールをクリアするメソッドであることが分かります。



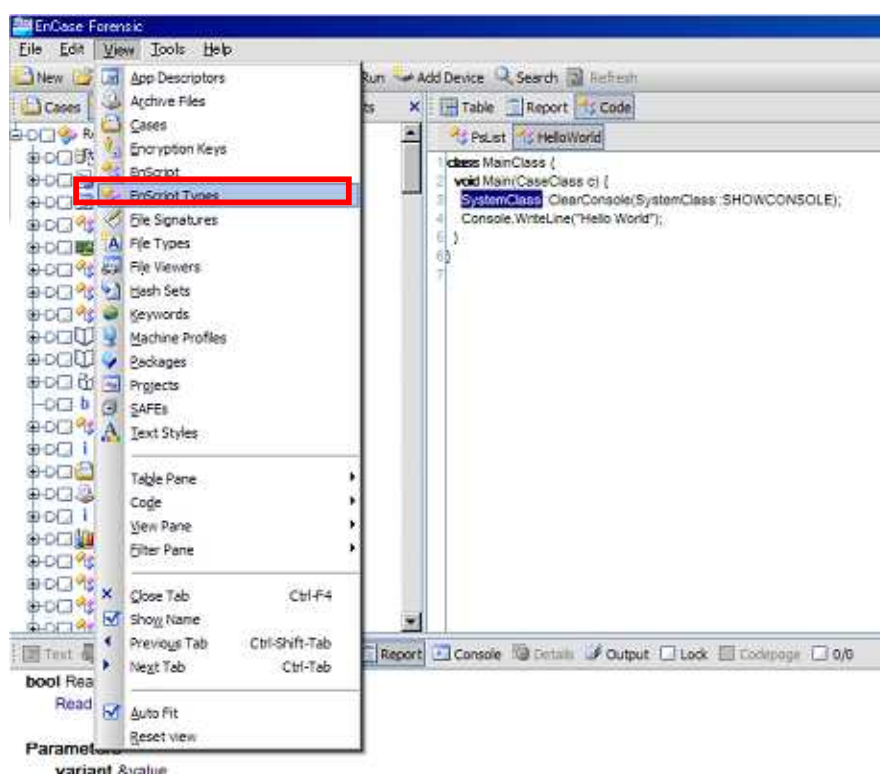
ちなみに、引数のオプションはメソッドの説明より上の部分にあります。

SystemClass Enumeration ClearConsoleOptions [Top]		
Name	Value	Description
SHOWCONSOLE	1	
KEEPCONSOLE	2	

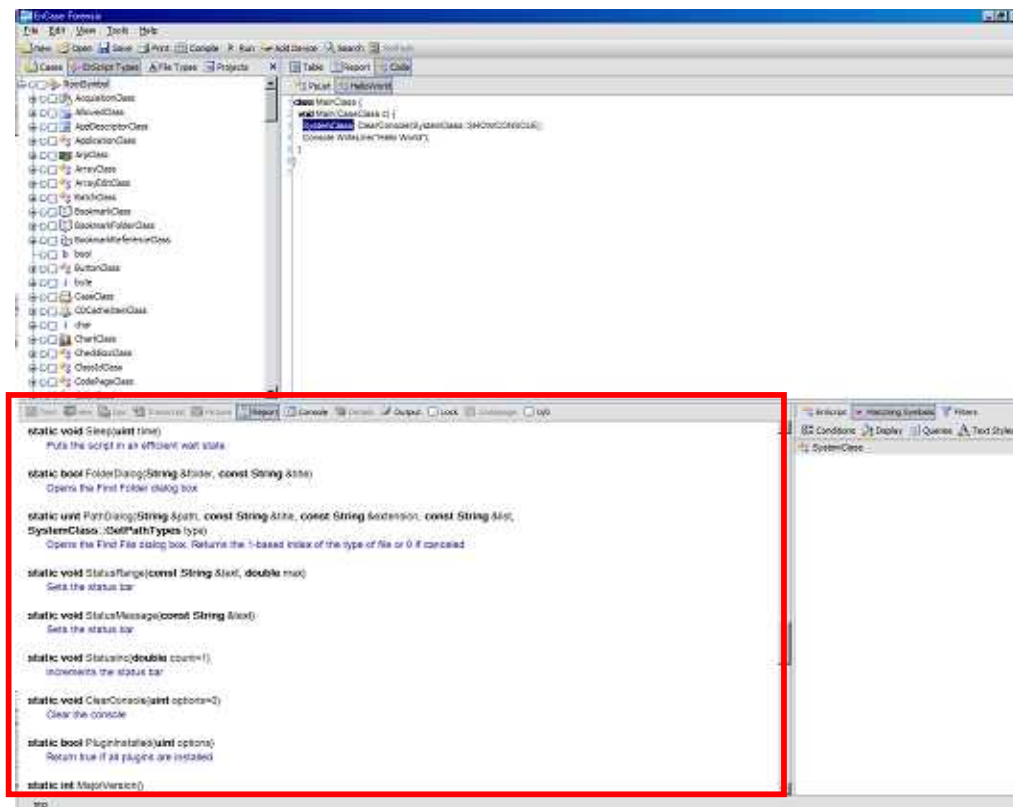
オプションの中に、SHOWCONSOLE が存在します。名前のとおりコンソールをクリアした後にコンソール画面を表示するオプションだろうと推測されます。

ヘルプで調べる方法以外に、EnScript の Code ビューで表示されているクラスやメソッドを簡単に調べる方法があります。

[View]メニューから[EnScript Types]を選びます。



そうすると、Tree ビューに EnScript のクラス群が表示されます。この状態で Code ビューにおいて調べたいクラスやメソッドをハイライトして F1 キーを押すと、レポートビューに説明が表示されます。EnCase 付属の EnScript や他人の書いた EnScript を読むときには便利です。



リファレンスの話はここまでにして、今回は EnCase に追加した証拠ファイル内の各ファイルのエントリの情報を表示するスクリプトを作りましょう。

エントリの情報にアクセスするには少なくとも2つのクラスを使用する必要があります。

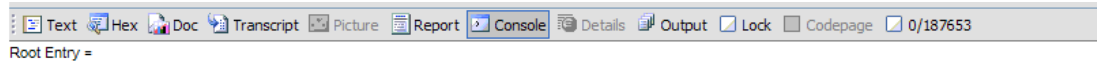
1. CaseClass
2. EntryClass

CaseClass の EntryRoot()メソッドを使うことで、ツリーペインのエントリビューにある最上位のエントリにアクセスすることができます。

```

class MainClass {
public:
    void Main(CaseClass c) {
        SystemClass::ClearConsole(1);
        EntryClass entry = c.EntryRoot();
        Console.WriteLine("Root Entry = " + entry.Name());
    }
};
    
```

EntryClass の名前は Name プロパティ (ヘルプで調べることで、NodeClass から継承していることがわかります) から得ることができます。このスクリプトを実行してみると、以下の画面になります。



なぜ名前が表示されないのでしょうか？ Output ビューにはエラーは表示されていないので、正常な動作のようです。

CaseClass の EntryRoot() によって参照されるルートエントリは、いわゆる「Entries」と表示されている部分であって、そこに追加した証拠ファイルなどのエントリはその下になります。よって、以下のように修正すれば追加した証拠ファイルやデバイスの名前を取得することができます。

```
class MainClass {
    void Main(CaseClass c) {
        SystemClass::ClearConsole(1);
        EntryClass entry = c.EntryRoot().FirstChild();
        Console.WriteLine("Root Entry = " + entry.Name());
    }
}
```

このように各エントリの FirstChild() メソッドや Next() メソッドを利用することで、全てのエントリをたどっていくことが可能ですが、特定のエントリをピンポイントで取得したいときには効率のよいやり方ではありません。

より効率的な方法の1つは、Find() メソッドを用いることです。このメソッドはファイル名を含むフルパスの情報から特定したエントリを取得します。

```
EntryClass entry = c.EntryRoot().Find("C:\boot.ini");
```

上記のコードでは、もし Find() メソッドで指定したパスもしくはファイル名が存在しない場合、実行時にエラーになってしまいます。



これを防ぐには、下記のように修正します。

```
if (EntryClass entry = c.EntryRoot().Find("C¥¥NoExist.ini"))  
    Console.WriteLine("Specific Entry = " + entry.Name());
```

今回は、EnScirpt でエントリにアクセスする方法を解説しました。エントリの特定のカラム(たとえばファイルサイズなど)に関する情報も、同じようなやり方で取得できます。

次回は、全てのエントリにアクセスして特定の条件にマッチしたエントリのみ表示する簡単なフィルタを作ります。

3. 製品・サービス紹介

「クイックリファレンスコース(eMail)」 (New)

Ji2 オリジナルトレーニングとして EnCase を使った調査をクイックリファレンスコースとして新設いたしました。今回新設したのはメールに関する半日コースです。本コースでは、EnCase フォレンジック版やエンタープライズ版でサポートされている電子メールアプリケーションの閲覧・検索など基本的な解析方法などについて取り扱います。対象としている電子メールアプリケーションは Outlook、Outlook Express が基本となり、ハンズオン形式で 1 人 1 台のノートパソコンを利用しながら行います。

内容は以下を予定しております。

(1)サポートされる電子メール形式とレコードビュー

(2)Outlook/Outlook Express への対応

(3)キーワード検索

-レコードビューにおける検索

-EML,MSG など単独ファイルの検索

-未使用領域の検索

(4)データ形式の変換/エクスポート

-Mbox データ形式

-その他の MUA

(5)その他の Artifacts

-Protected Storage 領域

URL : http://www.ji2.co.jp/training/encase/training_detail/index3.html

4. アップデート情報

EnCase プロダクト アップデート

EnCase Forensicバージョン 6.14(英語版)リリース: EnCase Forensicバージョン6.14がリリースされました。

新機能:

HP-UX ファイルシステムとサーブレット対応 - HP-UX システム上で動作するサーブレットを利用してマシンのスナップショット、プレビュー、取得が EnCase で可能。

HFS+ パーミッション対応 HFS+ (Mac OS 拡張ボリューム ハードドライブ・フォーマット) パーミッションに対応。

PGP Whole Disk Encryption(WDE)拡張対応 Windows Vista 64bit (64bit ADK 使用) と Mac OS 10.4 と 10.5 上で PGP WDE 暗号化されたデバイスの復号化をサポート。

Office 2007 サービスパック 2 対応

ZIP と RAR アーカイブ・ファイル拡張対応 - ZIP と RAR の解凍、復号化に対応する機能追加。

AOL Personal File Cabinet (PFC) 対応 AOL Personal File Cabinet データをパースし表示する作業をより速く強化。 インターネットのお気に入り、ダウンロードリンク、Buddy データ、およびアクセス番号データを追加。

Mozilla Firefox 3 アーチファクト対応 - インターネット履歴検索が強化されたことにより SQLite データベースに保持された Firefox アーチファクトをパースしレコードタブに表示。

LinEn 速度の改善

ProSuite FastBloc SE/SATA/IDE Vista 64bit 対応

メモリアクセス - 読み取るだけでもシステムクラッシュにつながることもある、ハードウェアデバイスで使用中のメモリを EnCase 物理メモリプレビュー範囲から除外することにより、滑らかなメモリ取得が可能。

EnCase Forensicバージョン 6.14.1(英語版)リリース: EnCase Forensicバージョン6.14.1がリリースされました。

新機能:

ソースプロセッサ: ソースプロセッサは EnScript の技術を利用して収集、分析、生成等の共通の調査作業を自動化 & 合理化。 EnCase プラットフォームを利用して、ソースプロセッサは、ローカルマシン上にある情報、ケースや証拠ファイル内にある異なるタイプの情報を分析。 現地

にあるマシンでも、ラボにあるマシンでも、電源が入っているマシンからでも切れているマシンからでもデータ収集できるスタンドアロン製品の EnCase Portable と動作します。収集ジョブがソースプロセッサ内で作成され、EnCase Portable にエクスポートされます。それからその EnCase Portable を使用して証拠を収集します。(収集結果を分析、レポートのために証拠は順々にソースプロセッサに取り込まれます。)

インストール: .ini ファイルのユーザカスタマイズを保存するために、EnCase はアップグレードのインストール中 Config ディレクトリ内のファイルを上書きせず。

レコード(記録): エントリメニューの新項目 **Tag Record** は、選択した項目に直接関連するすべての記録に青のチェックマークを設定可能。

EnCase eDiscoveryモジュール3.5(英語版)リリース: このバージョンはEnCase® Enterprise Version 6.13.10 and EnCase SAFE Version 6.13.4 (32bit)と適合します。

新機能:

Email 内の組み込みオブジェクト(OLE)対応: Lotus と Microsoft の E メールメッセージは、組み込みオブジェクトの検索可能。例えば、メッセージの本体に Excel のオブジェクトが挿入されている場合、この Excel オブジェクトが基準に沿っていればその E メールメッセージを収集。

Content Management サーバ: Content Management サーバ製品である2つの製品 (Microsoft SharePointとSymantec Enterprise Vault) が コマンドセンターのソースとして使用できるドキュメントレポジトリとして追加。

(1) **SharePoint:** 今回のリリースはSharePoint2003と2007のドキュメントライブラリにアクセスできる新規コネクタを含む。SharePoint コネクタはドキュメント、画像、フォーム、Wikiページ、データコレクション、スライドを含むドキュメントライブラリ、エリアライブラリ(リスト、掲示板、調査は含まず)から収集。ライブラリ内のすべてのドキュメントライブラリを検索(再帰的検索)する場合には、「Target All Libraries from Site」オプションを選択。

(2) **Symantec Enterprise Vault:** Enterprise Vault コネクタはMS ExchangeやLotus Domino内にあるシングルユーザーのメールアイテムや、ネットワークファイルサーバ内のファイルからの収集に対応。Enterprise Vaultへのアクセスのために新ソースを作成する場合には、Content Management Server カテゴリでソースタイプを選択でき、**Vault File System**もしくは**Vault Email**を選択。ここでの選択によってカストディアンとターゲットを決定する際に自動的にファイルシステムやEmailのユーザーリストをフィルタすることが可能。またVault collection jobsの出力タイプを証拠ファイル、もしくはロードファイルのいずれかより選択可能。

サンプル クライテリア: ECC3.5のインストールはサンプルクライテリアのフォルダを含む。このフォルダには、**Import Criteria** 機能でグローバルデータベースにインポートでき、すぐ使える条件やキーワードが含まれている。

Email コネクタ: Emailソースを作成し、Lotus Domino ver8.0 と 8.5から収集可能。

5. イベント情報

日本国内

・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: 2009年9月16日～17日 9時～18時予定

場所: 株式会社Ji2 セミナールーム

<http://www.ji2.co.jp/training/securityseminar/>

・eDiscoveryセミナー (LexisNexis後援) **New**

<http://www.ji2.co.jp/news/pdf/eDiscoveryOct07Rev1JP.pdf>

日時: 2009年10月7日(水) 10時～17時 (9時20分開場)

場所: コンファレンススクエア エムプラス (最寄駅: 東京駅)

対象: 知財部、法務部の皆様

<http://www.marunouchi-hc.jp/emplus/access/index.html>

・EnCase Computer Forensic トレーニング **受付中**

日時: 2009年11月10日～13日 9時～18時

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**

日時: 2009年11月16日～19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) **New**

日時: 2009年11月20日(金) 13時～18時 (5時間)

場所: 株式会社Ji2 セミナールーム

http://www.ji2.co.jp/training/encase/training_detail/index3.html

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

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/>
