

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2月号

はじめに

トヨタ自動車の世界市場で史上最大規模のリコール問題に直面し、米下院のエネルギー・商業委員会は2月25日に公聴会を開くと発表しました。これは、自動車メーカー日本第2位のホンダに、計100万台規模のリコール措置として波及しました。

トヨタのリコールに関しては、米国道路交通安全局(NHTSA)のデータとして、「過去10年間でトヨタ車の急加速に伴う死亡者数は19人に上り、他社すべてを合わせた件数の2倍近くに上る」と発表しました。そして、過去10年の急加速に関する消費者からの苦情など、すべての報告や、トヨタ内部の検討資料を提出するように要求。また、リコールに伴い、関連車種の販売と生産の一時停止を26日に決めるに至った、電子メールなど社内のすべてのやりとりなども提出を求めています。

米国では、今回のトヨタ自動車のリコールで要求されている、証拠開示(ディスカバリー)対応が昨今は常に必要となります。また今回のリコール騒ぎから、米国では日本企業全体の証拠開示体制(プロセス)を疑問視する声も上がっています。今後は、米国において日本企業全体へより厳しい姿勢が取られる可能性が考えられるため、より一層の日本企業における証拠開示要求対応が求められます。

内容

| | |
|---------------------|---|
| 1. 最新ビジネス・ニュース..... | 2 |
| 2. 調査チーム便り..... | 4 |
| 3. イベント情報..... | 6 |

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きます。本ガイドでは、eDiscovery対応手順の米国スタンダードを日本語でご紹介しております。入手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

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、ご遠慮なくお申し付けください。

1. 最新ビジネス・ニュース

Legal Tech in NY でのホットな話題

今年も2月1日から3日までニューヨークで開催されたリーガルテクノロジー最大のイベント、LegalTech NYに出展しました。昨年から続く不況の影響などにより参加人数の減少も予測されましたが、ふたを開けてみると予想を裏切る盛況ぶりでした。今回は、この熱い LegalTech で注目を集めた話題を幾つかご紹介いたします。



ECA

ここ数年コスト削減の手段として注目を集めている ECA は、今年もセミナーおよび展示ブースでの熱いトピックとなっていました。ECA= Early Case Assessment は、訴訟開始から2〜3か月以内に情報を分析し、案件のコストやリスク・メリットを早期に評価するプロセスを指します。これにより、膨大な時間やコストを費やす前に、和解すべきか、裁判に進めるべきかといった判断を戦略的に下すことができます。ECA 自体は従来から行われてきたプロセスであり、そのためのソリューションも数年来市場に出回っていますが、今年には特に不況によるコスト削減ニーズの高まりを受け、前後のプロセスとのシームレスな統合やユーザーフレンドリーなインターフェースを全面に押し出し、ECA 機能の強化や追加を謳うメッセージが各社で目に付きました。E ディスカバリーのコスト削減には欠かせない存在となりつつある ECA を備えているか、使いやすさはどうか、といった点が今後の E ディスカバリーソリューション選択の検討項目の一つとなりそうです。

Cloud

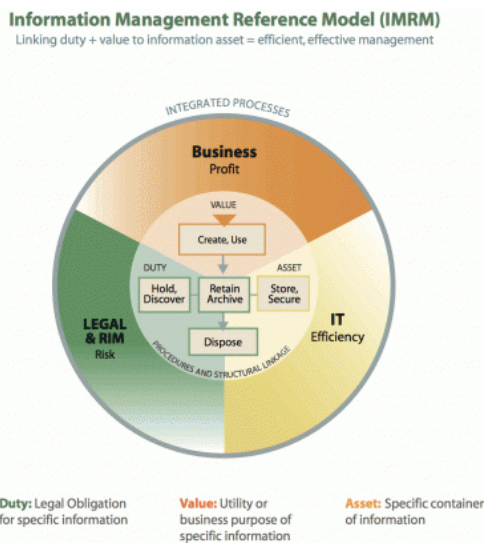
近年の流行キーワードである「クラウドコンピューティング」は LegalTech でも多くの注目を集めていました。リーガルテクノロジーにおけるクラウドには主に二つの側面があります。一つはリーガルツールとしてのクラウドサービス利用、もう一つはクラウド上のデータを開示する場合の対応です。様々なリーガルテクノロジーツールのクラウドモデル提供が進んでいる動きには、企業や法律事務所が不況によりコスト削減を迫られている背景があります。ケースマネジメントから訴訟ホールドの作成・管理、プロセッシングやレビューなど様々なツールをクラウドサービスとして利用することで、初期投資費用や維持費を削減するだけでなく、クラウドは E ディスカバリープロセスのインハウス化にも貢献します。すでにソーシャルメディアやクラウド上のデータからの証拠収集の判例は出てきていますが、これらには問題点も多く、Ji2 では今後の裁判所による解釈に注目していきます。

次世代のリーガルサーチ

毎年 LegalTech のメインスポンサーとして名を連ねる LexisNexis および Westlaw (Thomson Reuters)からはそれぞれ新しいリサーチソリューションの発表がありました。昨年の Google Scholar や Bloomberg Law の参戦を受け、リーガルリサーチ市場の競争は熾烈化の兆しが見られます。Thomson Reuters が Macbook Air を持ったデモスタッフを至る所に配備し、使いやすいユーザーインターフェースをアピールする一方、LexisNexis は Microsoft Office との統合を発表し、検索だけでなく業務効率の包括的な向上を目指す次世代ソリューションによる他製品との差別化を図っています。

IMRM

今や E ディスカバリーの国際基準ともいえる EDRM を提唱した EDRM グループからは、新たなモデルとして IMRM (Information Management Reference Model) が発表されました。IMRM は EDRM の最初のステップであるデータ管理を EDRM の一部かつ別個のプロセスとして新たに定義したもので、企業における文書サイクルを示すフレームワークとなっています。IMRM のプロセス自体は特に目新しいものではありませんが、改めてデータ管理の必要性を周知するという点で重要といえます。また、様々な部署や組織が関わる E ディスカバリーにおいて、部門間だけでなく、企業と社外の専門家や法律事務所などを繋ぐ共通言語としての役割も期待できます。



最後に

大きな盛り上がりを見せた LegalTech NY ですが、昨年のドイツ・フランスにおけるデータ保護に関する動きを受け注目を集めている EU だけでなく、アジアも含めたグローバルな E ディスカバリーに対する関心の高まりも印象的でした。アジア言語に対応するサービスやツールの増加はこうした関心とニーズ双方の高まりを象徴していると言えます。セミナーでも日本語 E ディスカバリーの話題が取り上げられるなど、2010 年もリーガルテクノロジーは益々グローバルなレベルでの発展を迎えそうです。また、企業・弁護士・専門家による連携が不可欠な E ディスカバリーにおいて、LegalTech は貴重な情報交換の場でもあります。訴訟の中心地であるニューヨークで最新の情報を入手する、それだけでも LegalTech は日本企業にとっても貴重な情報源となるのではないのでしょうか。

2. 調査チーム便り

1. FonreiscsAQ 公開中

Ji2 では EnCase の使い方や、フォレンジック調査に関連した日本語の FAQ (Frequently Asked Questions: 良くある質問) を取り纏め下記 URL にて公開しています。

<http://www.ji2.co.jp/forensics/ForensicsAQ/>

正式なサポート情報ではありませんが、Ji2 の調査チームでよく受ける質問や、自分たちで使う技術情報のメモも含めた Tips が記載してあります。EnCase FAQ のページでは EnCase の使用方法や機能に関する情報が 1 月 30 日時点で 100 件、フォレンジック調査全般に関するものが 50 件掲載されています。

詳細な技術情報までのご提供できておりませんが、内容は逐次更新しておりますのでご興味のある方はご参照いただければ幸いです。

2. 第一回 コンピュータフォレンジクス技術解説 セミナー資料公開中

昨年末12月4日に開催いたしました、Ji2調査チームによる「第一回 コンピュータフォレンジクス技術解説 無料セミナー」で利用した資料を、下記URLにて公開しています。

<http://www.ji2.co.jp/forensics/seminar.html>

第一回の技術解説セミナーでは、

1. 「Windows Memory Forensic Analysis」
2. 「RegDogによるレジストリHiveファイル解析」
3. 「Timeline Creation and Analysis」
4. 「EnCaseによる電子メール解析の基礎」

をテーマとして開催させていただきました。

それぞれのセッションで利用した資料のPDFバージョンをダウンロードしていただくことができます。

第二回は2月開催の予定でしたが、3月に開催される“コンピュータ・フォレンジクスI&II”トレーニング以降での実施を検討しております。詳細が決まりましたら、調査チームのWebページでアナウンスをさせていただきます。

3. VLICalculatorツール

ブラウザの履歴情報の保存ストレージや、スマートフォンのデータ管理用のストレージとしても利用されることが多いSQLiteデータベースですが、データ長を示す値などで“Variable Length Integer Format”を利用しています。

例えば1,000バイトのテキストデータがレコードに保存されている場合、この長さを示す値としては16進数で0x8F5Dという値がバイナリとして記録されることとなります。これをデコードするには、8F 5D →1000 1111 0101 1101→00 0111 1101 1101→0x7DD→2013→(2013 - 13) / 2 = 1,000byteとなるのですが、手動で計算するのは煩雑です。そこで、0x8F5Dを入力することで自動的に結果を出力する為のツールとしてVLICalculatorを調査チームのツールページ(<http://www.ji2.co.jp/forensics/tools/index.html>)で公開しています。

もし、SQLite3のタイプ値をデコードするのにお困りの方がいらっしゃいましたら、ぜひ使ってみていただければ幸いです。

4. クラッシュダンプ解析ツール

揮発性データであるメモリイメージをオフラインで解析するWindows向けツールとしてVolatility FrameworkやHBGary Responderなどがありますが、これらのツールはWindows 7やWindows Server 2008のような比較的新しいバージョンのOSの解析には対応していません。

単純なメモリのrawイメージではなくMicrosoftのクラッシュダンプ形式ファイルであればWinDbgのようなカーネルデバッガでそれらの解析が可能となりますが、デバッガとして実装された性質上、カーネルルートキットによって隠されたプロセスの情報などを見逃す可能性があります。

そこで、調査員がクラッシュダンプ形式のファイルからプロセス情報やカーネルモジュール情報を網羅的に抽出するEnCaseプラグインのスクリプト(EnScript)を作成して公開しております。

<http://cci.cocolog-nifty.com/blog/>

5. EnScript Tutorial

弊社の過去のニュースレターではEnScriptプログラミングの基礎知識を取り上げております。EnScriptのコーディングに関する情報は世界的に見ても解説しているサイトが非常に少ないのですが、以下のサイトでもEnScriptのチュートリアルを公開しています。英語で書かれておりますが、興味のある方は是非一読をお勧めいたします。

<http://www.forensickb.com/2007/09/enscript-tutorial-part-i.html>

6. EnCase Enterprise eDiscoveryモジュール

Version3.8では以下の拡張が行われております。

- Symantec Enterprise Vault V8 SP4用コネクタ

Symantec Enterprise Vault導入企業様へのグッドニュースです。アーカイブツールとして国内での導入実績が多い「Symantec Enterprise Vault」に接続するためのコネクタが、eDiscoveryモジュールに追加されました。

Version4の新機能もアナウンスされており、以下の追加がございます。

- Legal Hold
- Pre-collection Analytics
- Identification, Preservation, and Collection
- Processing, Analysis, and Early Case Assessment
- First-Pass Review

3. イベント情報

日本国内

- **EnCase Computer Forensic I トレーニング**
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)**
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
<http://www.ji2.co.jp/seminar/encase/schedule.html>

- **EnCase Computer Forensic II トレーニング**
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**
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
<http://www.ji2.co.jp/seminar/security/schedule.html>

- **データリカバリートレーニング 受付中 (締切3/5)**
日時: 2010年3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/data-recovery/schedule.html>

■ 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/>
