

Ji2 ニュースレター (フォレンジック / インシデント・レスポンス)

2009 年 2 月号

はじめに

昨今、世界的な景気後退局面で企業合併・買収が盛んになっておりますが、これらの場面でもフォレンジック技術が使われていることを皆様はご存知でしょうか。金融業界で言うデューデリジェンス(Due Diligence:適正評価手続き)において、近年では投資先や被買収企業の事業活動全般を調査対象とし、ビジネス面、財務経理面、資金調達面、法契約面でコンピュータ上のビジネス・データについて調査が行われます。電子データの普及で身近になってきたフォレンジックは、今後も多岐多様化して進化を遂げていくと考えられ、弊社でもそうしたニーズに合わせたサービスの展開を行って参ります。

目次

1. 最新ビジネスのニュース	2
2. テクニカルニュース	3
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	7
5. イベント情報	8

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。コンピュータ・セキュリティのインシデント対応「Computer Security Incident Response (CSIR)」の為のベスト・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、CSIRのベスト・プロセスとそのプロセス構築のサポート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、情報漏洩対応、コンピュータ調査、フォレンジック、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

最新ビジネス・ニュース

シマンテックと Ji2 企業向け法的証拠の電子情報開示ソリューション[eDiscovery]の提供で協業

2008 年 12 月 8 日、株式会社シマンテック（以下シマンテック、代表取締役社長：加賀山進）と株式会社 Ji2（代表取締役社長：藤澤哲雄）は、日本企業向けの法的証拠電子開示に関するコンサルティングサービスを協業して提供していく旨発表致しました。

シマンテックと Ji2 は本協業において、両社の専門分野とノウハウを活用し、法的な対応が必要となった企業のメールシステム、サーバ、データベースなど企業内の IT インフラに存在する膨大な量のデータに対して洗い出しや監査を行います。これにより、企業は電子文書や電子メールおよび知財データなど法的証拠として有効性のあるデータの迅速かつ的確に収集することが可能となります。国際的に企業に求められるセキュリティおよびコンプライアンスの要求がより厳しくなる中、デジタル・フォレンジックならびに eDiscovery（電子情報開示）と呼ばれるソリューションのニーズが高まっております。これらのソリューションは、パソコンやサーバ、ネットワーク機器など、企業の IT 資産において不正アクセスや機密情報漏洩などコンピュータに関する犯罪、PL 法や知的財産などの法的紛争、会計監査などの際に、必要なデータや電子的記録を迅速に収集/分析し、その法的な証拠性を保全・開示を行うサービスとなっております。近年、日本国内においても、法的リスクへの対策ならびに海外とのビジネスで求められる要件として、本ソリューションに対する注目が高まっております。

シマンテックと Ji2 はこのたび両社のコアコンピテンスを活かし、協力して日本国内における eDiscovery の導入に関するコンサルティングサービスの提供を開始致します。具体的には、Ji2 は、本分野におけるグローバルでの豊富な実績を活かし、法的証拠の収集および分析において求められる固有のノウハウを提供致します。一方シマンテックは、これまで日本国内の金融、製造、情報通信業界等の大規模な環境において、ストレージやセキュリティ、コンプライアンスに関わる IT 基盤の設計および構築や、情報のセキュリティ保護に関わるセキュリティポリシーの設計、監査支援など、幅広い経験と実績を基盤にしたコンサルティングサービスを提供致します。

両社は日本国内においてこれらのサービスを通じ、海外とのビジネス上迅速かつ効果的な訴訟対応が求められるグローバル企業をはじめとして、より能動的に訴訟リスクへの対応を目指す国内企業への効果的な支援活動を目指します。

1. テクニカルニュース

揮発性データ収集のトレンド

コンピュータ・フォレンジックの鉄則として OOV(Order Of Volatility)というものがあります。これは失われやすい証拠を優先して取得するというポリシーを表したものです。コンピュータ上のデータには CPU レジスタやメモリ、ハードディスクのデータがありますが、証拠取得はレジスタ、メモリ、ディスクの順で取得される必要があります。

例えば、PC がマルウェアに感染した場合、そのマルウェアは外部のサーバと通信を行っている場合があります。しかしそのような証拠はメモリ上にしか残らないため、メモリ上のデータを取得する前に電源を切ってしまうと、重要な手がかりを見逃してしまうことにつながりかねません。

これまでの証拠取得の対象はほとんどディスクのみであることが多く、メモリのデータを取得した場合もその全体のメモリイメージから文字列を抽出する程度の調査に限定されていましたが、最近ではメモリ解析技術の向上により、詳細なメモリデータ解析が可能になってきています。

メモリイメージのフォーマットとツールの紹介

メモリ調査において、調査員は、ディスクと同様にまず実行中のメモリ上のデータを全てイメージとして取得して、次にツールを使ってそのイメージを解析していきます。現在、調査対象としてメジャーな OS である Windows OS のメモリイメージに関しては、主に以下の 3 つの種類があります。また、ツールにはメモリイメージをダンプするツールと、そのイメージを調査するツールの 2 種類があります。

イメージのフォーマット	長所	短所	ツールの例
物理メモリのローイメージファイル： 物理メモリに現在マッピングされているデータをそのままダンプしたファイル	対応しているツールが最も多く調査手法も成熟	CPU レジスタの値を操作する rootkit により特定のメモリ領域が隠蔽される可能性あり	調査ツール： Volatility Framework , PTFinder, HBGary Responder ダンプツール： Win32dd, MDD, FastDump (HBGary のダンプツール)
クラッシュダンプファイル： (OS が深刻なエラーに陥った状態、いわゆるブルースクリーン時において生成されるイメージファイル)	物理メモリの情報だけでなくデバッグに必要な CPU レジスタの情報を含む	API の制限から取得できないメモリ領域が存在する	調査ツール： Volatility Framework, WinDbg] ダンプツール： Win32dd

<p>ハイバネーションファイル: (ノートPCなどでハイバネーションが起きた際にストアされるイメージファイル)</p>	<p>ハイバネーション状態からレジュームするため必要となるCPUレジスタの情報を含む</p>	<p>レジューム後に収集したファイルの場合、イメージの最初の1ページ分のサイズを上書きしてしまう (forensically soundではない)</p>	<p>調査ツール: Volatility Framework, Sandman Framework ダンプツール: 専用のツールはなし (EnCaseなどを使ってコピーを実行)</p>
--	--	---	---

メモリー解析ツールの今と未来

これまで、ネットワークの接続状態など揮発性データについては、netstatのようなユーザプログラムをCD-ROM上から起動するなどして収集していたため、カーネルルートキットの情報隠蔽に対しては無効でした。メモリーイメージそのものを直接パースして解析するやり方であれば、そのような隠蔽を検出できる可能性があります。また、ファイルシステム上に存在しないメモリー上のデータやドライバを調査するケースでは、メモリーイメージが唯一の証拠になると考えられます。

ただし、メモリーをダンプするタイミングで工夫すれば、誤ったメモリーイメージを取得させることができるため、その結果をすべて信頼するのではなく、あくまで証拠の一つとして考えるべきです。

どのメモリーイメージフォーマットにも一長一短があります。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については、物理メモリーのローイメージファイルに比べるとCPUレジスタの情報を含む反面、対応している調査ツールが現時点では少なく、そのインターフェースのユーザビリティにも課題があります。また、どの3つのメモリーフォーマットも、ディスクにスワップアウトされたメモリーデータを格納している「ページファイル」のデータを含まないため(特にクラッシュダンプファイルは生成時にページファイルの内容を上書きしてしまいます。)、物理メモリーの内容だけでなくページファイルも同時に取得して調査できるようになれば、揮発性データの調査精度はさらに上がっていくと思われます。

2. 製品・サービス紹介(Legal Tech 展示会にて)

Legal Tech 2009 が 2009年2月2日から4日まで Hilton New York Hotel で開催されました。Legal Techではカンファレンスの他に展示会があり、様々な製品やサービスの紹介がされていました。ここではその一部についてご紹介致します。

レビュープラットフォーム製品に関して

ほとんどのプラットフォーム製品が多言語つまり UNICODE 対応を予定している(CT Summation /Concordance など)か、対応済み(Clearwell など)になってきています。なかでも、STRATIFY は他に比べると日本特有の圧縮フォーマットにも対応しており、日本語での eDiscovery との相性が良い製品です。

使いやすさの観点から言うと、Clearwell 社のレビュープラットフォームは Ajax などの google ベースのテクノロジーを採用することで1操作あたりのステップ数を少なくしており、使いやすい印象があります。また、Clearwell の特徴である「Transparent Search」と呼ばれるキーワード検索時にマッチした単語一覧を表示してくれる機能も利便性を高めています。

興味深い機能として、iConnect 社の「Concept Search」機能があります。Concept Search は違う単語でも同じ意味を表すものであれば関係ある単語とみなすサーチ方法です。例えば、「terminating」で検索した際には、「firing」も結果に表示することができます。ただ、単なるキーワードサーチに比べるとこのような新機能は弁護士からの信頼をまだ受けておらず、業務ではあまり使われていないのが現状のようです。

Autonomy 社のレビューツールは Link Map という custodian 同士の結びつきを表示する機能を持っています。この機能を使うことで、訴訟案件に関係した custodian の特定が容易になります。現在は mail のみに対応しています。

レビュープラットフォーム製品の今後の傾向としては、各国のコードページへの対応や、現在は未対応のファイルフォーマット(Lotus Notes のデータベースファイルなど)内のキーワード検索の可否などがあり、それらをどの程度カバーできているかが製品選定のポイントになりそうです。

Index Engines について

Index Engines 社のレビュープラットフォームはインデックス処理のパフォーマンスにおいて他社のレビュープラットフォームとは一線を画しています。毎秒 2 ギガビットのデータをインデックス化することができ、インデックスデータのサイズはオリジナルのディスクサイズのわずか 8%です。たとえばテープバックアップシステムのディスカバリでは、50%から 70%の時間の節約が可能になるそうです。この高速化は従来の Internet サーチエンジンのようにすべての情報をインデックスするのではなく、訴訟に関係する responsive data のみをインデックス化する技術により実現されています。

nexidia 社の Audio Discovery サービスについて

nexidia 社が「Nexidia Audio Discovery OnDemand」というサービスを実施しています。従来、Audio Discovery は人が聞き取って原稿化するという人的にも時間的にもリソースの消費を強いる作業だっ

たのですが、nexidia 社は独自の技術で入力した検索対象のテキストの音声を高速かつ確実に audio ファイルの中からサーチすることができ、目的のデータを効率的に収集することができます。この技術は「North American のしゃべる言葉は音声パターンとして分類した場合、40 程度のパターンのみに限定することができる」という実験結果をもとに構築されているそうです。以下のサイトでデモを見ることができますので是非ご覧ください。

<http://www.nexidia.com/solutions/legal>

3. 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 6.12.1(英語版)リリース: EnCaseバージョン6.12.1がリリースされました。

新機能 :

LinEn Command Line追加

Internet history Internet historyについて修正されました。

Export to Mail Format .msgにExportした際、フォルダ構造を保存できず、間違った場所にファイルがExportされることについて修正されました。

Keyword Search New KeywordダイアログボックスにUTF8のオプションがないことについて修正されました。

Records レコードタブのサーチヒットカラムに誤った結果が表示されることについて修正されました。
また他のファイルをクリックした際にヒットタブが更新されないことについて修正されました。

4. イベント情報

日本国内

- EnCase Computer Forensic I トレーニング
日時: 2009年3月10日～13日 9時～18時
場所: 株式会社Ji2 セミナールーム
- データリカバリートレーニング
日時: 2009年4月22日～24日 9時～18時
場所: 株式会社Ji2 セミナールーム
- HBGary Windowsライブメモリ・フォレンジックスとマルウェア解析トレーニング
日時: 2009年5月～6月頃開催予定(詳細はWebにてご確認下さい)
場所: 株式会社Ji2 セミナールーム

米国

- Legal Tech 2009
日時: 2009年2月2日～4日
場所: The Hilton New York Hotel
- Ji2 Data Recovery Seminer 2009
日時: 2009年4月8日～10日
場所: Cypress, CA

-
- このニュースレターは、お申し込みをいただいた方へ配信しております。
 - 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 東京都新宿区四谷 4 丁目 3 番地 802 号

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

※オフィス拡大のため 2 月 15 日からは下記住所に移転いたします。

〒160-0022 東京都新宿区新宿 1-9-5 大台ビル 3F
