

Ji2 ニュースレター (フォレンジック / eDiscovery)

2009年4月号

はじめに

昨今の世界的な景気後退局面において、米国では大規模な不祥事の増加により、行政によるデータ提出要請、コンプライアンス監査、および州・連邦レベルでの調査が増えています。それに比例してeDiscoveryの市場も25%-30%の年成長率で増え、3年後の2012年には5,000億円の市場規模を超えると米国ガートナー社は予想しています。

そうした中、米国大手フォレンジック関連企業の顔ぶれを見ると、全てがeDiscoveryビジネスを中心としたビジネスモデルに変身しており、弊社米国パートナーのガイダンスソフト社も”これからはフォレンジックではなくeDiscoveryの分野で勝負する！”と言い切るほど裁判対応サポートビジネスが旬です。

今後のフォレンジック・ビジネスはeDiscovery市場の一部として存在するのは米国だけか、それとも日本も訴訟技術 (Legal Technology) がビジネスとして急速発展するかは、この数年で判断できるでしょう。

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	4
3. 製品・サービス紹介 (Legal Tech 展示会にて)	4
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。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 eDiscovery 費用が莫大なパテント・トロール (Patent Troll)とは

パテント・トロールとは、自らが保有する特許権を侵害している疑いのある企業を見つけ出し、自身は当該特許に基づく製品やサービスを提供してしないにも関わらず、巨額の賠償金やライセンス料を得ようとする者を指す俗称です。日本では特許ゴロなどと呼ばれます。パテント・トロールで数十億円のお金を得て引退する個人の話を聞くことがありますが、ほとんどの場合、公的な市場から何億ドルもの資金を調達するために、法人または LLC として弁護士と情報資源を豊富に持つ専門家チームで構成されます。

パテント・トロールは悪いこと？

パテント・トロールで使われる特許の多くは、特許侵害者を見つけても、訴訟を起こす資金や法的手段を持たない小規模なベンチャー企業や個人発明家から取得されます。そういう意味では、弱者を救済し、開発者を初期段階で保護してイノベーションを活性化するとして、パテント・トローリングを正当化する意見もあります。しかしその反面、巨額の賠償金目当てで安価に特許権を買い集め、いつでも特許権侵害訴訟を起こせるように特許ポートフォリオの拡充に努めている会社もあるため、その区別は非常に曖昧なのが現状です。

日本企業がパテント・トロールの攻勢に弱い理由

パテント・トロールはハイテク・IT 分野の訴訟に多く、日本企業は特許率も高く、関連製品・サービスを世界で展開しているため、IP 訴訟の格好のターゲットとなります。また、E ディスカバリーに不慣れな点もこれを助長していると言えます。

一般の特許侵害訴訟とパテント・トローリングの違い

これまで、日本企業の特許侵害訴訟の多くは、同業界の企業間(例えば自動車メーカー同士や電機メーカー同士)で争われてきました。そのため、他社に自社特許侵害の疑いがあっても、逆に相手方の有する特許権の侵害で反撃されるリスクがあるため深く追求できなかつたり、ライバル企業であっても何らかの取引関係があることが多いため、互いに不利益になる紛争は避け、友好的にライセンス料の交渉を行ったり、クロスライセンス契約を結んだりして円満な解決を図る傾向がありました。

一方、パテント・トローリングでは、原告(パテント・トロール)は自ら製造やサービス提供を行わないため、敗訴の場合でもビジネス中止に追い込まれるリスクがありません。対する被告側の企業は、訴訟が長引くだけでも製品開発計画に狂いが出る、顧客に不安を与え販売に悪影響が出る、社内の人材が訴訟対応に追われ本来の業務に支障が出る、といった多くのリスクを抱えています。このため、このような弱みに付け込んだパテント・トロールの法外な要求に屈せざるを得ないということもしばしば起こりうるのです。

まとめ: IP 訴訟(パテント・トローリング)の E ディスカバリー対応

3つの訴訟形態のうち訴訟コストが特に高いのが IP 訴訟です。電子証拠の開示要求が多岐にわたり、賠償額が数百億円以上であれば、数十億円をかけて開示を実施する事もしばしばあります。中でも、パテント・トローリングは上記のような理由で多額の訴訟費用が掛かる可能性があり、慎重な対応が必要です。弊社が最近経験したケースでは、パテント・トロールが原告となり、日本企業に特許侵害賠償を求めてきました。この時の E ディスカバリー費用は数億円にもなりましたが、適切な対応の結果、有利に裁判を進めることができました。日本企業が巻き込まれたパテント・トローリングの案件に関わり、証拠開示(E ディスカバリー)の対応を見誤ると、多大な代償を払わなければならないということを改めて実感しました。そのよ

うな事態を避けるため、これまで紹介してきたコスト削減のポイントを実施し、効果的な E ディスカバリー対応準備で、狙われやすい IP を始めとする訴訟に備えてください。

EnCase の検索技術が連邦地方裁判所によって有効と認められる

ガイダンスソフトウェア社(NASDAQ:GUID)は、2009年3月23日に、EnCaseソフトウェアがすでに持っている強い法的地位を更に高める判決を得ました。この訴訟では、電子的に格納された情報(ESI)を確認、検索、収集するのに用いられる EnCase のネイティブ検索エンジンについて焦点が向けられ、法廷は原告、被告の双方から広範囲な証拠を考慮し、EnCase で実行された詳細な検索分析に基づく情報を有効なものとして認めました。

Smith v. Slifer Smith & Frampton/Vail Associates Real Estate訴訟

民事訴訟当事者が、eDiscovery要求の期限が迫った状態で、不適切にハードディスクデータ消去したことがアメリカ連邦地方裁判所で認められました。裁判所によると、関連したESIを求めて被告のノートパソコンを調べるために、原告によってEnCaseが使われました。法廷で引き合いに出されたEnCase検索手順は、社会保障番号、クレジットカード番号、知的所有権、あるいは、この訴訟のようにデータワイプの証拠のようなデータパターンを特定するために、他の検索キーワードと同様に複雑なキーワードを使用することができるとの事です。

EnCaseによって維持されたデータが証拠として有効であると法廷は判決を下しました。以前から多くの裁判がEnCaseの収集、保存、認証能力を有効とする一方で、今回の決定では、民事訴訟におけるeDiscovery関連の問題においても、分析目的で利用されるEnCase検索エンジンを有効と認めています。

*Guidance Softwareは、Socha-Gelbmann's 2008 Electronic Discovery SurveyにおけるeDiscoveryソフトウェアプロバイダの中で最高位(Top5プロバイダ)の評価を受けました。またEnCase eDiscoveryのデータ収集および2次処理能力について、Law Technology Newsから2つの2008 アワードを受賞しました。

<http://investors.guidancesoftware.com/releasedetail.cfm?ReleaseID=372241>

2. テクニカルニュース

EnCase と F-Response を組み合わせる

フォレンジック調査や eDiscovery の現場では、時々システムの電源を落とすことができない状況が発生することがあります。例えばシステムを停止してしまうとハードディスク全体が暗号化された状態になり、EnCase からアクセスしてもデータ内容を読むことができないといった場合などです。(EnCase では EDS モジュールでサポートされている暗号化ドライブであれば、オフラインの状態からでもデータへのアクセスが可能になります)

EnCase エンタープライズ版では、稼働中のシステム上でサブレットと呼ばれるクライアントプログラムを実行し、ネットワーク経由でハードディスクの内容にアクセスすることが可能です。この場合 Windows や Linux といった OS の上で動作するサブレットはハードディスク全体の暗号化の影響を受けずに、暗号化が解除された状態のセクタへアクセスすることが可能になります(暗号化ソリューションによってはこの方法でも依然として暗号化したデータにアクセスすることができない場合があります)

同様にネットワーク経由で稼働中システムのハードディスクへリモートからアクセスを可能にするソリューションとして、F-Response (<http://www.f-response.com/>) があります。

F-Response は通信プロトコルとして iSCSI を利用しており、ターゲットの PC に接続されているハードディスクを、あたかも(調査員が使うフォレンジック PC に接続された)ローカルのハードディスクであるかのようにアクセスすることができます。そして、フォレンジック的には重要なことですが、F-Response はターゲットのハードディスクへのフォレンジック PC からのアクセスに対してライトブロック機能を提供してくれます。F-Response を利用した場合には、以下の手順を実行することになります。

1. ターゲットシステムへ管理者権限でログオン
2. ターゲットシステム上で F-Response クライアントプログラムを実行
3. クライアントからライセンスサーバと接続し認証
4. ターゲットシステム上で iSCSI 通信ポート(3260/tcp)をオープン
5. フォレンジック PC 上の iSCSI イニシエータからターゲットへ接続
6. フォレンジック PC でターゲットハードディスクをマウント

フォレンジック PC には、事前にマイクロソフトの iSCSI イニシエータープログラムをインストールしておく必要があります。(Windows Vista などは標準機能)

フォレンジック PC にターゲットシステムのハードディスクを接続したら、後は EnCase を起動し Add Device をすればローカルハードディスクとしてターゲットのハードディスクがめでたく表示されます。後はいつもの通り EnCase を利用してターゲットシステムのハードディスクを保全することや、調査することができます。ただし、ターゲットは稼働中システムですので、時間をかけているとハードディスクの内容が変化していく点には注意が必要です。

他にも幾つか注意しなければいけない点がありますが、まず EnCase エンタープライズの仕組みと違い、認証はユーザー名とパスワードによるものとなります。また、特にロール(権限)の概念はないので、設定されたユーザー名とパスワードがわかると、その先のアクセス制御の仕組みはありません。

またデータ通信の暗号化は標準では実施されていないため、通信経路上の暗号化が必要となるケースでは、IPsec を使って暗号化を行うなど別の処理が必要となります。しかし、クロスケーブルを使いターゲットとフォレンジック PC 間を 1 対 1 で接続し、通信経路の安全性が確認できる状況であれば、あえて暗号化を行う必要はないかもしれません。

逆にターゲットのハードディスクが TrueCrypt や Windows Vista の BitLocker などハードディスク全体の暗号化が実施されているケースでは、暗号化ソフトウェアにより対応が異なります。例えば TrueCrypt でハードディスク全体が暗号化されている場合には、特に意識することなく EnCase と F-Response の組み合わせでハードディスクの内容にアクセスすることができますが、Vista BitLocker で暗号化されているボリュームでは、EnCase からハードディスクをマウントする際に (EDS モジュールを通じて) 鍵情報を求められることとなります。また、TrueCrypt や PGP が持つ機能として暗号化ファイルを仮想ドライブとしてマウントしているようなケースでは、F-Response のターゲットドライブとしてそれらの仮想的にマウントされたドライブを確認することはできないようです。(最新版の 3.09 では論理ボリューム単位でのマウントにも対応するようになりましたが、残念ながら TrueCrypt や PGP ディスクなどで仮想ドライブとしてマウントされた論理ボリュームは扱うことができないようです)

F-Response を使った場合の、データ転送速度ですが、クロスケーブルにて 1 対 1 で接続した場合には、以下の条件では 80GB の保全で約 4.5 時間が必要となります。ただし 100BASE-T での接続ですので、1000Gbps での接続であればより早い時間での保全が可能となります。

参考転送速度:

HDD:SATA 3.5', 7,500 回転 容量 80GB、100BASE-T(100Mbps)
80GB 転送時間→4 時間 35 分(275 分)、転送速度 291MB/分

F-Response の現在のバージョンでは、ターゲットとして利用可能な OS は基本的に Windows シリーズ (Windows 2000、XP、Vista、Windows Server) が対象となります。しかし、4 月 15 日にリリースされたバージョン 3.09 では Linux と Apple Mac OS X がサポート対象となっています。Linux や Mac OS X の対応バージョンなど詳しくはメーカーの Web でご確認ください。

興味深い使い方としては、F-Response クライアントを実行するターゲットは Windows ですが、そこに接続するフォレンジック PC は必ずしも Windows である必要はなく、iSCSI を利用可能な OS (例えば Mac OS X など) であれば、ターゲット上で実行されている F-Response クライアントに接続し、ターゲットのハードディスクへのアクセスが可能となります。また、最新版のバージョン 3.09 では、32bit 版の Windows については物理メモリ (RAM) の内容についてもダンプが可能になっています。今後はメモリイメージの取得などにも F-Response が利用可能になるかもしれません。むしろ F-Response で取得したメモリイメージの解析は HBGary Responder などを使う必要が出てきますが、リモート・フォレンジックツールを利用して、メモリダンプを取得できるようになる機会は今後益々増えることになると予想されます。

EnCase Forensic 版と F-Response を組み合わせることで、通常では対応できないケースにも対応が可能になる可能性があります。EnCase ユーザーで興味のある方は評価版などを使って検証されてみてはいかがでしょうか。

3. 製品・サービス紹介

Forensic Dossier (ドシエ)

2008年12月号にてLogicube社のDossier(以下、ドシエ)をご紹介いたしましたが、今回はその追加情報をご紹介します。米国ではForensicコピー機としてはトップシェアを獲得しているLogicube社が新たに発売した製品ですが、ようやくメーカーサイドでもホームページにて紹介を始めました。

http://www.logicubeforensics.com/products/hd_duplication/dossier.asp

そしてこの春、新たな機能やオプションが加えられますので以下にご紹介いたします。

(1)SAS および SCSI サポート

発売当初はIDE、SATA対応のみでしたが、SAS および SCSI もサポートするようになりました。

(2)リトライ回数の設定

Bad セクターの読み込みリトライ回数を1~998の範囲で設定し、任意の回数をリトライさせることができるようになります。任意設定できるようになった事で、不要にハードディスクを痛めることが避けられるようになりました。

(3)ビープ音

データキャプチャ完了をビープ音で知らせる機能が追加されます。またエラー時には異なるビープ音がアラートとして2分間またはユーザがドシエのインターフェースを通して止めるまで続きます。エラー時に音で知らせてくれるので、コピー中に機械に張り付いている必要がありません。

(4)ドライブ拡張

1台の大きなサイズのHDDから2台のHDDにコピーすることができます。ただし、2台のコピー先HDDの合計サイズは1台のコピー元HDDサイズよりも大きい必要があります。例えば750GBのHDDを500GBのHDD×2台にコピーができます。

(5)ATA パスワードの設定および除去

従来、他の製品と組み合わせなければ対応できなかったハードディスクパスワード解除機能が追加された事で、パスワードがかかったディスクのコピーも可能になりました。

(6)コピー先 HDD の暗号化

(7)Apple マックコンピュータに対応

AppleコンピュータのデータキャプチャをPCインターフェース経由でできるようになります。

(8)バッテリーパック

再利用可能なバッテリーパックを追加で購入できるようになります。

4. アップデート情報

EnCase プロダクト アップデート

EnCase Enterprise バージョン 6.13(英語版) およびField Intelligence Model バージョン 6.13(英語版)リリース: EnCase EnterpriseおよびField Intelligence Modelバージョン6.13がリリースされました。

新機能:

Auditor Permission (View All Logs) 新しいユーザパーミッション「View All Logs」は、ユーザにSAFEログをReadすることを可能にします。このパーミッションでSAFEにログオンしたユーザはキーマスターのようにログを見ることができます。

SAFE Backups SAFEバックアップは、リカバリーのためのコアファイルを保存できるようになります。

Delayed Loading of Internet Artifacts EnCaseはインターネットアーチファクトおよびCaseロード後の別々のスレッドとして関連したデータを解析できるようになります。

PDF Support プリントダイアログはファイルをPDFフォーマットで保存するオプションを提供します。

Enhanced Vista BitLocker Support EnCaseはデータボリュームの解析や自動ロック解除メカニズムを使用する拡張版BitLockerをサポートするようになりました。

Enhanced CREDANT Mobile Guardian Support CREDANT Mobile Guardian (CMG) 6.0.2をサポートします。

PGP Whole Disk Encryption (WDE) Support 適切なPGP証明書があれば、EnCaseはPGP暗号化ディスクからデータを検索し収集できるようになりました。

Tableau Write Blocker Support 書き込み防止装置のTableauをサポートします。

(ご注意)もしEnCase eDiscoveryまたはEnCase Data AuditとPolicy Enforcement (バージョン3.1以上)を現在利用されているようでしたら、eDiscoveryまたはData Auditインストーラーに付属するEnCaseのバージョンを使い続けてください。

EnCase Forensic バージョン 6.13(英語版)リリース: EnCase Forensicバージョン6.13がリリースされました。

新機能:

Delayed Loading of Internet Artifacts EnCaseはインターネットアーチファクトおよびCaseロード後の別々のスレッドとして関連したデータを解析できるようになります。

PDF Support プリントダイアログはファイルをPDFフォーマットで保存するオプションを提供

します。

Enhanced Vista BitLocker Support EnCaseはデータボリュームの解析や自動ロック解除メカニズムを使用する拡張版BitLockerをサポートするようになりました。

Enhanced CREDANT Mobile Guardian Support CREDANT Mobile Guardian (CMG) 6.0.2をサポートします。

PGP Whole Disk Encryption (WDE) Support 適切なPGP証明書があれば、EnCaseはPGP暗号化ディスクからデータを検索し収集できるようになりました。

Tableau Write Blocker Support 書き込み防止装置のTableauをサポートします。

5. イベント情報

日本国内

- EnCase Computer Forensic I トレーニング
日時: 2009年6月2日～5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年秋頃開催予定
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: 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 II トレーニング
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

米国

- CEIC 2009
日時: 2009年5月17日～20日
場所: Orland, FL

- Legal Tech West Coast 2009
日時: 2009年6月24日～25日
場所: Los Angeles, CA

■ 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/>
